COMMAND REFERENCE GUIDE

Extreme SLX-OS Command Reference, 18s.1.02

Supporting the ExtremeSwitching SLX 9140 and SLX 9240 Switches

9036144-00
May 2019

Copyright © 2019 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, please see: www.extremenetworks.com/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: www.extremenetworks.com/support/policies/software-licensing

Contents

Preface **27**
- Conventions 27
  - Notes, cautions, and warnings 27
  - Text formatting conventions 27
  - Command syntax conventions 28
- Documentation and Training 28
  - Training 28
- Getting Help 28
  - Subscribing to Service Notifications 29
- Providing Feedback to Us 29

About This Document **31**
- Supported hardware and software 31
- What's new in this document 31
  - New commands 31
  - Modified commands 31
  - Deprecated commands 32

Using the SLX-OS CLI **33**
- User accounts 33
- Accessing the CLI 33
- Command modes 34
  - Privileged EXEC mode 34
  - Global configuration mode 34
  - Using the do command as a shortcut 34
  - Using the top command as a shortcut 34
- Displaying CLI commands and command syntax 35
- Completing CLI commands 36
- CLI keyboard shortcuts 36
- Using CLI command output modifiers 37
- Debug and system diagnostic commands 37
- Command shortcuts (aliases) 37
  - Configuring global aliases 37
  - Configuring user-level aliases 38

Commands A - B **39**
- aaa accounting 39
- aaa authentication 41
- action 43
- action python-script 45
- action-timeout 47
- activate (telemetry collector) 48
- activate (telemetry server) 49
- activate (VXLAN gateway) 50
- add (telemetry) 51
- add destination 52
- address-family l2vpn evpn (BGP) 54
- address-family unicast (BGP) 55

advertise dot1-tlv 57
advertise dot3-tlv 58
advertise-backup 59
advertise optional-tlv 60
advertisement-interval (VRRP) 62
advertisement-interval-scale 64
aggregate-address (BGP) 65
alias 67
alias-config 69
allow-vn-tag 70
always-compare-med 71
always-propagate 72
announce-interval 73
announce-timeout 75
area authentication (OSPFv3) 76
area nssa (OSPFv2) 78
area nssa (OSPFv3) 80
area prefix-list (OSPFv2) 82
area range (OSPFv2) 84
area range (OSPFv3) 86
area stub (OSPFv2) 88
area stub (OSPFv3) 90
area virtual-link (OSPFv2) 92
area virtual-link (OSPFv3) 94
area virtual-link authentication (OSPFv3) 96
arp 98
arp access-list 100
as-path-ignore 102
auth-port 103
auto-cost reference-bandwidth (OSPFv2) 104
auto-cost reference-bandwidth (OSPFv3) 106
auto-shutdown-new-neighbors 108
backup-advertisement-interval 109
banner 110
basedn 111
bfd 112
bfd holdover-interval 114
bfd interval 116
bfd shutdown 118
bgp-redistribute-internal 119
breakout mode 120
bridge-domain 122
bridge-domain (EVPN) 123
bridge-priority 125
bsr-candidate 127

Commands C - D 129

capability as4-enable 129
capture packet interface ethernet 130
cee 132
cee-map default 133

certutil import sshkey 134
channel-group 136
chassis 138
chassis fan airflow-direction 140
cisco-interoperability 141
class 142
class-map 143
clear arp 144
clear bgp evpn neighbor 145
clear bgp evpn routes 146
clear bgp evpn routes type 147
clear counters 148
clear counters access-list 150
clear counters link-fault-signaling 152
clear counters storm-control 154
clear dot1x statistics 156
clear ip arp inspection statistics 157
clear ip arp suppression-cache 158
clear ip arp suppression-statistics 159
clear ip bgp dampening 160
clear ip bgp flap-statistics 161
clear ip bgp local routes 162
clear ip bgp neighbor 163
clear ip bgp routes 165
clear ip bgp traffic 166
clear ip dhcp relay statistics 167
clear ip igmp groups 168
clear ip igmp statistics 169
clear ip ospf 170
clear ip route 172
clear ipv6 bgp dampening 173
clear ipv6 bgp flap-statistics 174
clear ipv6 bgp local routes 175
clear ipv6 bgp neighbor 176
clear ipv6 bgp routes 178
clear ipv6 bgp traffic 179
clear ipv6 counters 180
clear ipv6 dhcp relay statistics 181
clear ipv6 mld groups 182
clear ipv6 mld statistics 183
clear ipv6 nd suppression-cache 184
clear ipv6 nd suppression-statistics 185
clear ipv6 neighbor 186
clear ipv6 ospf 187
clear ipv6 route 189
clear ipv6 vrrp statistics 190
clear lacp 192
clear lacp counters 193
clear lldp neighbors 194
clear lldp statistics 195

clear mac-address-table 196
clear policy-map-counters 198
clear ptp counter interface 200
clear spanning-tree counter 201
clear spanning-tree detected-protocols 203
clear statistics bridge-domain 205
clear statistics vlan 206
clear tunnel statistics 207
clear vrrp statistics 208
CLI 210
client 213
client-interface 214
client-interfaces-shutdown 215
client-isolation-strict 216
client-to-client-reflection 217
clock set 218
clock timezone 219
cluster 220
cluster management node-id 221
cluster management virtual 222
cluster-control-vlan 224
cluster-id 225
cluster-system-id 226
compare-med-empty-aspath 227
compare-routerid 228
confederation identifier 229
confederation peers 230
configure terminal 231
connector 232
continue 233
copy 234
crypto ca authenticate 237
crypto ca enroll 239
crypto ca import 241
crypto ca trustpoint 243
crypto key 244
dampening 246
database-overflow-interval (OSPFv2) 248
database-overflow-interval (OSPFv3) 249
debug access-list-log buffer 250
debug arp packet buffer 251
debug dhcp packet buffer 253
debug dot1x packet 255
debug ip bgp 257
debug ip bgp neighbor 259
debug ip igmp 261
debug ipv6 bgp 263
debug ipv6 bgp neighbor 265
debug lacp 267
debug lldp dump 269

debug lldp packet 271
debug spanning-tree 273
default-information-originate (BGP) 275
default-information-originate (OSPFv2) 276
default-information-originate (OSPFv3) 278
default-local-preference 280
default-metric (BGP) 281
default-metric (OSPF) 282
default-passive-interface 283
delay 284
delay-link-event 285
delay-request-min-interval 287
delete 289
deny inner-gtp-https 290
deploy 291
description (event handler) 292
description (interfaces) 293
description (LLDP) 294
description (STP) 295
description (TVF domain) 296
description (VRRP) 298
designated-forwarder-hold-time 299
destination 300
df-load-balance 301
dhcp ztp cancel 302
dhcp ztp log 304
diag burninerrclear 307
diag portledtest 309
diag portloopbacktest 311
diag setcycle 320
diag systemverification 322
diag turboramtest 324
dir 326
disable (LLDP) 329
distance (BGP) 330
distance (OSPF) 331
distribute-list prefix-list (OSPFv3) 333
distribute-list route-map 334
domain 335
dot1x authentication 336
dot1x enable 337
dot1x port-control 338
dot1x quiet-period 340
dot1x reauthenticate 341
dot1x reauthentication 342
dot1x reauthMax 343
dot1x test eapol-capable 344
dot1x test timeout 346
dot1x timeout 347
duplicate-mac-timer (EVPN) 349

Commands E - F **351**
efa debug clear-config 351
efa deploy 352
efa device credentials update 353
efa execution show 354
efa fabric configure 356
efa fabric deconfigure 358
efa fabric setting show 360
efa fabric setting update 364
efa fabric setting 367
efa fabric show 368
efa supportsave 369
enable (PTP) 370
encoding (Telemetry) 372
encryption-level 373
endpoint-tracking enable 374
endpoint-tracking timeout reauth-period 375
enforce-first-as 376
error-disable-timeout enable 377
error-disable-timeout interval 378
esi auto lacp 380
event-handler 381
event-handler abort action 383
event-handler activate 384
evpn 387
evpn irb ve 388
extend bridge-domain 389
extend vlan 391
external-lsdb-limit (OSPFv2) 392
external-lsdb-limit (OSPFv3) 393
fast-external-fallover 394
fec mode 395
firmware activate 397
firmware commit 398
firmware download 399
firmware download ftp 402
firmware download interactive 404
firmware download scp 406
firmware download sftp 408
firmware download tftp 410
firmware download usb 412
firmware recover 414
firmware restore 415
flow 416
forward-delay 418

Commands G - J **421**
graceful-restart (BGP EVPN) 421
graceful-shutdown 423
gtp-de-encapsulation 425
hardware 426

hello (LLDP) 427
hello-time 429
hold-time 431
host 432
host-table aging-mode conversational 433
host-table aging-time conversational 434
http server 435
insight enable 437
install-igp-cost 439
instance 440
interface (telemetry) 442
interface ethernet 444
interface loopback 445
interface management 446
interface port-channel 447
interface ve 448
interval 449
interval (telemetry) 450
ip access-group (general) 451
ip access-group (overlay) 453
ip access-list 455
ip address 457
ip address (VXLAN) 459
ip anycast-address 460
ip arp-aging-timeout 461
ip arp inspection 463
ip arp inspection filter 464
ip arp inspection trust 465
ip arp learn-any 467
ip as-path access-list 468
ip community-list extended 469
ip community-list standard 470
ip dhcp relay address 472
ip dhcp relay gateway address 473
ip dhcp relay information option 474
ip dns 475
ip icmp rate-limiting 476
ip icmp redirect 477
ip igmp snooping enable 478
ip igmp snooping fast-leave 479
ip igmp snooping last-member-query-count 480
ip igmp snooping last-member-query-interval 481
ip igmp snooping mrouter interface 482
ip igmp snooping querier enable 483
ip igmp snooping query-interval 484
ip igmp snooping query-max-response-time 485
ip igmp snooping restrict-unknown-multicast 486
ip igmp snooping robustness-variable 487
ip igmp snooping startup-query-count 488
ip igmp snooping startup-query-interval 489

ip igmp snooping static-group....490
ip interface....491
ip mtu....493
ip ospf active....495
ip ospf area....496
ip ospf auth-change-wait-time....497
ip ospf authentication-key....498
ip ospf bfd....499
ip ospf cost....500
ip ospf database-filter....501
ip ospf dead-interval....503
ip ospf hello-interval....504
ip ospf md5-authentication....505
ip ospf mtu-ignore....507
ip ospf network....508
ip ospf passive....510
ip ospf priority....511
ip ospf retransmit-interval....512
ip ospf transmit-delay....513
ip policy route-map....514
ip port (telemetry)....515
ip prefix-list....517
ip proxy-arp....519
ip receive access-group....520
ip route....522
ip route static bfd....524
ip route static bfd holdover-interval....526
ip router-id....528
ip vrrp-extended auth-type....529
ipv6 access-group (general)....531
ipv6 access-group (overlay)....533
ipv6 access-list....535
ipv6 address....537
ipv6 anycast-address....539
ipv6 anycast-gateway-mac....540
ipv6 dhcp relay address....542
ipv6 dns....544
ipv6 icmpv6 rate-limiting....545
ipv6 mld snooping enable....546
ipv6 mld snooping fast-leave....547
ipv6 mld snooping last-member-query-count....548
ipv6 mld snooping last-member-query-interval....549
ipv6 mld snooping mrouter interface....550
ipv6 mld snooping querier enable....551
ipv6 mld snooping robustness-variable....552
ipv6 mld snooping static-group interface....553
ipv6 mld snooping startup-query-count....554
ipv6 mld snooping startup-query-interval....555
ipv6 mtu....556
ipv6 nd cache expire....557

ipv6 ospf active 558
ipv6 ospf area....559
ipv6 ospf authentication ipsec....560
ipv6 ospf authentication ipsec disable....561
ipv6 ospf authentication spi....562
ipv6 ospf bfd 564
ipv6 ospf cost....565
ipv6 ospf dead-interval....566
ipv6 ospf hello-interval 567
ipv6 ospf hello-jitter....568
ipv6 ospf instance....569
ipv6 ospf mtu-ignore....570
ipv6 ospf network....571
ipv6 ospf passive....573
ipv6 ospf priority....574
ipv6 ospf retransmit-interval....575
ipv6 ospf suppress-linklsa....576
ipv6 ospf transmit-delay....577
ipv6 policy route-map....578
ipv6 prefix-list....579
ipv6 protocol vrrp....581
ipv6 protocol vrrp-extended....582
ipv6 receive access-group....583
ipv6 route....585
ipv6 route next-hop-vrf....587
ipv6 route null....589
ipv6 route static bfd 591
ipv6 route static bfd holdover-interval 593
ipv6 router ospf....594
ipv6 vrrp-extended auth-type....595
ipv6 vrrp-extended-group....596
ipv6 vrrp-group 597
ipv6 vrrp-suppress-interface-ra....598
iterations....599

Commands K - M....601

key....601
key-add-remove-interval....603
key-rollover-interval....604
keypair....605
lacp default-up 606
lacp port-priority 607
lacp system-priority 608
lacp timeout 609
ldap-server host 611
ldap-server maprole 613
license eula....614
line vty exec-timeout 616
link-fault-signaling rx 618
lldp profile 620
load-balance (default mode)....621

load-balance (NPB mode) ... 623
local-as ... 625
log (OSPFv2) ... 626
log (OSPFv3) ... 628
log-dampening-debug ... 630
log-shell ... 631
logging auditlog class ... 632
logging raslog console ... 633
logging raslog console stop ... 634
logging syslog-client ... 635
logging syslog-facility local ... 636
logging syslog-server ... 637
logical-interface ... 639
loopback phy ... 641
mac access-group (general) ... 642
mac access-group (overlay) ... 644
mac access-list extended ... 646
mac access-list standard ... 648
mac-address-table ... 649
mac-address-table mac-move detect ... 652
mac-address-table mac-move limit ... 653
map ... 654
map bridge-domain (VXLAN gateway) ... 656
map cos ... 658
map dscp ... 660
map traffic-class ... 662
map vlan (VXLAN gateway) ... 664
map vni auto (VXLAN gateway) ... 666
master-vlan (STP) ... 667
match access-group ... 668
match as-path ... 669
match community ... 670
match extcommunity ... 671
match interface ... 672
match ip address acl ... 673
match ip address prefix-list ... 674
match ip next-hop prefix-list ... 675
match ip route-source prefix-list ... 676
match ipv6 address acl ... 677
match ipv6 address prefix-list ... 678
match ipv6 next-hop prefix-list ... 679
match ipv6 route-source prefix-list ... 680
match mac address acl (NPB) ... 681
match metric ... 682
match protocol ... 683
match route-type ... 684
match tag ... 685
match uda address acl ... 686
match vrf ... 687
max-age ... 688

maxas-limit ... 690
maximum-paths (BGP) ... 691
maximum-paths (eBGP, iBGP) ... 693
maximum-paths (OSPF) ... 695
max-metric router-lsa ... 696
max-metric router-lsa (OSPFv3) ... 698
max-route ... 700
med-missing-as-worst ... 701
member-vlan (STP) ... 702
metric-type ... 703
minimum-links ... 704
mode (LLDP) ... 705
monitor session ... 706
mtu ... 707
multipath ... 709
multiplier (LLDP) ... 711

Commands N - Q ... 713

neighbor activate ... 713
neighbor advertisement-interval ... 715
neighbor allowas-in ... 717
neighbor as-override ... 719
neighbor bfd ... 721
neighbor capability as4 ... 723
neighbor capability orf prefixlist ... 725
neighbor default-originate ... 727
neighbor description ... 728
neighbor ebgp-btsh ... 730
neighbor ebgp-multihop ... 732
neighbor enable-peer-as-check ... 734
neighbor encapsulation ... 736
neighbor enforce-first-as ... 738
neighbor filter-list ... 740
neighbor graceful-shutdown ... 742
neighbor local-as ... 744
neighbor maxas-limit in ... 746
neighbor maximum-prefix ... 748
neighbor next-hop-self ... 750
neighbor next-hop-unchanged ... 752
neighbor password ... 753
neighbor peer-group ... 755
neighbor prefix-list ... 757
neighbor remote-as ... 759
neighbor remove-private-as ... 761
neighbor route-map ... 763
neighbor route-reflector-client ... 765
neighbor send-community ... 767
neighbor shutdown ... 769
neighbor soft-reconfiguration inbound ... 771
neighbor static-network-edge ... 773
neighbor timers ... 775

neighbor unsuppress-map 777
neighbor update-source 779
neighbor weight 781
network 783
next-hop-enable-default 785
next-hop-recursion 786
npb policy route-map 787
ntp authentication-key 788
ntp server 790
ntp source-ip 792
oscmd 793
overlay-class-map 795
overlay-gateway 797
overlay-policy-map 799
overlay-service-policy 801
overlay-transit 803
owner 804
password-attributes 806
pbf destination 808
pbf destination-group 809
peer (MCT) 810
peer-interface 811
permit ip host 812
police cir 814
police-remark-profile 816
policy-map 818
port 820
port-channel path-cost 821
preempt-mode 823
priority 824
priority1 826
priority2 827
priority-group-table 828
priority-table 830
profile (LLDP) 832
profile (telemetry) 833
profile ipv6-lookup 835
profile overlay-visibility 837
profile route-table 839
profile tcam 841
protocol 844
protocol lldp 845
protocol ptp 846
protocol spanning-tree 848
protocol vrrp 850
protocol vrrp-extended 851
ptp-vlan 852
pw-profile 854
python 856
qos cos 860

qos cos-mutation 862
qos cos-traffic-class 863
qos cpu 864
qos drop-monitor enable 865
qos dscp-cos 866
qos dscp-mutation 867
qos dscp-traffic-class 868
qos flowcontrol 869
qos map cos-dcsp 871
qos map cos-mutation 872
qos map cos-traffic-class 873
qos map dscp-cos 875
qos map dscp-mutation 876
qos map dscp-traffic-class 877
qos map traffic-class-cos 878
qos map traffic-class-dscp 879
qos map traffic-class-mutation 880
qos random-detect traffic-class 881
qos red profile 883
qos service-policy 885
qos trust 886
qos tx-queue limit 888
qos tx-queue scheduler strict-priority 889
queue 891

Commands R - Sh 893

radius-server host 893
rate-limit 895
rd (EVPN VLAN/BD) 897
redistribute 898
region 901
reload 902
reload (DiagOS) 904
remap lossless-priority 905
remove destination 906
rename 907
resequence access-list 908
resource-monitor cpu enable 910
resource-monitor memory enable 911
resource-monitor process memory 912
retain route-target all 914
retries 915
retries (Telemetry) 916
revision 917
rfc1583-compatibility (OSPF) 918
rib-route-limit 919
rmon alarm 921
rmon collection history 923
rmon collection stats 925
rmon event 926
role name 928

root access console....930
root enable....931
route-map (default system-mode)....932
route-map (NPB)....934
route-target (EVPN VLAN/BD)....937
router bgp....939
router ospf....940
router-interface....941
rule....942
seq (deny/permit rules in UDAs)....944
seq (overlay class map)....946
seq (rules in IPv4 extended ACLs)....948
seq (rules in IPv4 standard ACLs)....953
seq (rules in IPv6 extended ACLs)....955
seq (rules in IPv6 standard ACLs)....960
seq (rules in MAC extended ACLs)....962
seq (rules in MAC standard ACLs)....965
seq overlay-class....967
service password-encryption....969
service-policy....970
set (policer)....972
set as-path....973
set automatic-tag....974
set comm-list....975
set community....976
set dampening....977
set distance....979
set extcommunity....980
set interface (NPB route-maps)....982
set interface (PBF destination)....984
set local-preference....986
set metric....987
set metric-type....988
set next-hop-tvf-domain....989
set origin....991
set tag....992
set weight....993
sflow collector....994
sflow enable (global version)....996
sflow polling-interval (global version)....997
sflow sample-rate (global version)....998
sflow source-interface....999
shape....1001

Show A through Show I....1003

show access-list....1003
show access-list-log buffer....1006
show access-list-log buffer config....1008
show arp....1009
show arp access-list....1011
show bfd....1012

show bfd neighbors....1014
show bfd neighbors application....1016
show bfd neighbors dest-ip....1018
show bfd neighbors details....1020
show bfd neighbors interface....1023
show bgp evpn neighbors....1025
show bgp evpn neighbors advertised-routes....1026
show bgp evpn neighbors routes....1029
show bgp evpn routes....1032
show bgp evpn routes type igmp-join-sync....1033
show bgp evpn routes type igmp-leave-sync....1034
show bgp evpn summary....1035
show bridge-domain....1036
show capabilities....1038
show capture packet config....1040
show capture packet interface ethernet....1041
show cee maps....1042
show cert-util ldapca....1043
show cert-util sshkey....1044
show cert-util syslogca....1045
show chassis....1046
show cipherset....1048
show cli....1049
show clock....1050
show cluster....1051
show cluster management....1053
show copy-support status....1054
show cpu-interface....1055
show crypto ca....1056
show crypto key....1058
show debug arp packet....1059
show debug dhcp packet....1061
show debug dhcp packet buffer....1062
show debug ip bgp all....1065
show debug ip igmp....1066
show debug ipv6 mld....1067
show debug ipv6 packet....1068
show debug lacp....1070
show debug lldp....1071
show debug spanning-tree....1072
show debug vrrp....1073
show defaults threshold....1074
show diag burninerrshow....1076
show diag burninstatus....1077
show diag revision....1079
show diag setcycle....1080
show diag sysinfo....1081
show dot1x....1082
show environment fan....1088
show environment history....1089

show environment power 1091
show environment sensor 1092
show environment temp 1093
show event-handler activations 1094
show file 1096
show firmwaredownloadhistory 1097
show firmwaredownloadstatus 1098
show hardware profile 1100
show hardware profile overlay-visibility 1105
show history 1106
show http server status 1107
show inner-gtp-https 1108
show interface 1109
show interface port-channel 1113
show interface stats 1114
show interface status 1117
show inventory 1118
show ip anycast-gateway 1120
show ip arp inspection 1121
show ip arp inspection interfaces 1123
show ip arp inspection statistics 1125
show ip arp suppression-cache 1127
show ip arp suppression-statistics 1129
show ip arp suppression-status 1131
show ip as-path-list 1133
show ip bgp 1134
show ip bgp attribute-entries 1135
show ip bgp dampened-paths 1136
show ip bgp filtered-routes 1137
show ip bgp flap-statistics 1138
show ip bgp neighbors 1140
show ip bgp neighbors advertised-routes 1143
show ip bgp neighbors flap-statistics 1144
show ip bgp neighbors last-packet-with-error 1145
show ip bgp neighbors received 1146
show ip bgp neighbors received-routes 1147
show ip bgp neighbors rib-out-routes 1149
show ip bgp neighbors routes 1151
show ip bgp neighbors routes-summary 1152
show ip bgp peer-group 1153
show ip bgp routes 1154
show ip bgp routes community 1157
show ip bgp summary 1158
show ip community-list 1159
show ip dhcp relay address interface 1160
show ip dhcp relay statistics 1161
show ip igmp groups 1162
show ip igmp snooping 1164
show ip igmp static-groups 1165
show ip igmp statistics vlan 1166

show ip interface 1167
show ip interface brief 1169
show ip ospf 1170
show ip ospf area 1171
show ip ospf border-routers 1173
show ip ospf config 1174
show ip ospf database 1175
show ip ospf filtered-lsa area 1178
show ip ospf interface 1179
show ip ospf neighbor 1181
show ip ospf redistribute route 1182
show ip ospf routes 1183
show ip ospf summary 1185
show ip ospf traffic 1186
show ip ospf virtual link 1187
show ip ospf virtual neighbor 1188
show ip prefix-list 1189
show ip route 1190
show ip route-map 1193
show ipv6 anycast-gateway 1194
show ipv6 bgp 1195
show ipv6 bgp attribute-entries 1196
show ipv6 bgp dampened-paths 1197
show ipv6 bgp filtered-routes 1198
show ipv6 bgp flap-statistics 1199
show ipv6 bgp neighbors 1201
show ipv6 bgp neighbors advertised-routes 1203
show ipv6 bgp neighbors flap-statistics 1205
show ipv6 bgp neighbors last-packet-with-error 1206
show ipv6 bgp neighbors received 1207
show ipv6 bgp neighbors received-routes 1208
show ipv6 bgp neighbors rib-out-routes 1210
show ipv6 bgp neighbors routes 1211
show ipv6 bgp neighbors routes-summary 1212
show ipv6 bgp peer-group 1215
show ipv6 bgp routes 1216
show ipv6 bgp routes community 1219
show ipv6 bgp summary 1220
show ipv6 counters interface 1221
show ipv6 dhcp relay address interface 1222
show ipv6 dhcp relay statistics 1223
show ipv6 interface 1224
show ipv6 mld groups 1226
show ipv6 mld snooping 1227
show ipv6 mld statistics 1229
show ipv6 nd 1230
show ipv6 nd suppression-cache 1232
show ipv6 nd suppression-statistics 1234
show ipv6 nd suppression-status 1236
show ipv6 neighbor 1238

show ipv6 ospf 1240
show ipv6 ospf area 1241
show ipv6 ospf database 1242
show ipv6 ospf interface 1244
show ipv6 ospf memory 1245
show ipv6 ospf neighbor 1246
show ipv6 ospf redistribute route 1248
show ipv6 ospf routes 1249
show ipv6 ospf spf 1250
show ipv6 ospf summary 1251
show ipv6 ospf virtual-links 1252
show ipv6 ospf virtual-neighbor 1253
show ipv6 prefix-list 1254
show ipv6 route 1255
show ipv6 static route 1257
show ipv6 vrrp 1258

Show J through Show Z 1265

show lacp 1265
show license 1266
show link-fault-signaling 1268
show link-fault-signaling counters 1269
show lldp 1270
show lldp interface 1271
show lldp neighbors 1272
show lldp statistics 1274
show mac-address-table 1275
show mac-address-table endpoint-tracking 1278
show media 1280
show media interface 1282
show media optical-monitoring 1283
show monitor 1285
show netconf 1286
show netconf capabilities 1287
show netconf client-capabilities 1288
show netconf datastores 1290
show netconf files 1291
show netconf schemas 1292
show netconf sessions 1293
show netconf statistics 1294
show netconf-state datastores 1295
show notification stream 1296
show ntp status 1297
show overlay-class-map 1298
show overlay-policy-map 1299
show overlay-service-policy 1300
show packet-encap-processing 1302
show pbf destination 1304
show pbf destination-group 1306
show policy-map 1308
show port port-channel ethernet 1310

show port-channel 1311
show port-channel detail 1313
show port-channel summary 1314
show port-security 1315
show process cpu 1317
show process info 1319
show process memory 1321
show ptp brief 1323
show ptp clock 1324
show ptp clock foreign-masters record 1325
show ptp corrections 1326
show ptp parent 1327
show ptp port interface 1328
show ptp time-property 1331
show qos cpu queue 1332
show qos flowcontrol interface 1335
show qos interface all 1337
show qos interface ethernet 1338
show qos interface port-channel 1340
show qos maps cos-traffic-class 1341
show qos maps dscp-cos 1342
show qos maps dscp-mutation 1343
show qos maps dscp-traffic-class 1344
show qos maps traffic-class-cos 1345
show qos maps traffic-class-dscp 1346
show qos maps traffic-class-mutation 1347
show qos red profiles 1348
show qos red statistics 1349
show qos tx-queue interface 1350
show rmon 1351
show rmon history 1353
show route-map 1354
show running-config 1356
show running-config aaa 1357
show running-config aaa accounting 1359
show running-config arp 1360
show running-config event-handler 1362
show running-config interface port-channel 1364
show running-config ip access-list 1365
show running-config ip receive 1366
show running-config ip route 1367
show running-config ipv6 1368
show running-config ipv6 access-list 1371
show running-config ldap-server 1373
show running-config mac access-list 1374
show running-config password-attributes 1375
show running-config radius-server 1377
show running-config rmon 1379
show running-config role 1380
show running-config rule 1381

show running-config snmp-server ... 1383
show running-config ssh ... 1384
show running-config ssh server ... 1385
show running-config ssh server key-exchange ... 1386
show running-config telemetry collector ... 1387
show running-config telemetry profile ... 1388
show running-config telemetry server ... 1390
show running-config tvf-domain ... 1391
show running-config username ... 1392
show sflow ... 1394
show span path session ... 1396
show spanning-tree ... 1397
show ssh client status ... 1399
show ssh server status ... 1400
show startup-config ... 1401
show startup-database ... 1403
show statistics access-list ... 1404
show statistics bridge-domain ... 1406
show statistics vlan ... 1407
show storm-control ... 1409
show support ... 1411
show system ... 1412
show system internal dcm ... 1413
show system internal nsm ... 1417
show system internal nsx ... 1419
show system internal ovsdb ... 1421
show system monitor ... 1423
show telemetry client-cert ... 1424
show telemetry collector ... 1425
show telemetry server status ... 1427
show telnet server status ... 1428
show threshold monitor ... 1429
show tpvm ... 1431
show tunnel ... 1432
show tunnel statistics ... 1434
show users ... 1436
show version ... 1437
show vlan ... 1439
show vlan brief ... 1441
show vlan classifier ... 1443
show vlan private-vlan ... 1444
show vlan rspan-vlan ... 1445
show vrf ... 1446
show vrrp ... 1448

Commands Shu - Z ... 1455

shutdown (interface) ... 1455
shutdown (STP) ... 1457
site ... 1458
snmp-server access-enable vrf ... 1460
snmp-server community ... 1462

snmp-server contact ... 1463
snmp-server context ... 1465
snmp-server enable trap ... 1467
snmp-server engineid local ... 1468
snmp-server group ... 1469
snmp-server host ... 1471
snmp-server location ... 1473
snmp-server mib community-map ... 1474
snmp-server sys-descr ... 1475
snmp-server user ... 1477
snmp-server v3host ... 1480
snmp-server view ... 1482
snmp trap link-status disable ... 1484
source ... 1487
source-ip ... 1489
span session ... 1490
spanning-tree autoedge ... 1491
spanning-tree bpdu-mac ... 1492
spanning-tree cost ... 1493
spanning-tree edgeport ... 1494
spanning-tree guard root ... 1496
spanning-tree link-type ... 1497
spanning-tree portfast ... 1498
spanning-tree priority ... 1500
spanning-tree restricted-role ... 1501
spanning-tree restricted-tcn ... 1502
spanning-tree shutdown ... 1503
speed (Ethernet) ... 1504
speed (LAG) ... 1506
ssh ... 1508
ssh client cipher ... 1511
ssh client cipher non-cbc ... 1512
ssh client key-exchange ... 1513
ssh client mac ... 1514
ssh server cipher ... 1515
ssh server cipher non-cbc ... 1516
ssh server key ... 1517
ssh server key-exchange ... 1519
ssh server mac ... 1520
ssh server rekey-interval ... 1521
ssh server shutdown ... 1522
start-shell ... 1524
static-network ... 1526
statistics (bridge domain) ... 1527
statistics (VLAN) ... 1528
statistics-enable ... 1529
storm-control ingress ... 1530
strip-802-1br ... 1532
strip-vn-tag ... 1534
strip-vxlan ... 1536

summary-address (OSPFv2) ... 1538
summary-address (OSPFv3) ... 1540
suppress-arp ... 1542
suppress-nd ... 1543
switch-attributes ... 1544
switchport ... 1546
switchport access ... 1547
switchport mode ... 1548
switchport mode trunk-no-default-native ... 1549
switchport port-security ... 1550
switchport port-security mac-address ... 1551
switchport port-security max ... 1552
switchport port-security shutdown-time ... 1553
switchport port-security sticky ... 1554
switchport port-security violation ... 1555
switchport trunk allowed ... 1557
switchport trunk default-vlan ... 1559
switchport trunk native-vlan-untagged ... 1560
switchport trunk native-vlan-xtagged ... 1561
switchport trunk tag native-vlan ... 1563
sync-interval ... 1564
sysmon sfm-walk ... 1566
system packet-timestamp egress ... 1567
system packet-timestamp ingress valid ... 1569
system-description ... 1570
system-mode ... 1571
system-monitor ... 1573
system-monitor-mail ... 1576
system-name ... 1578
table-map ... 1579
tacacs-server ... 1581
telemetry client-cert ... 1584
telemetry collector ... 1585
telemetry profile ... 1586
telemetry server ... 1590
telnet ... 1591
telnet server ... 1593
terminal ... 1595
threshold-monitor cpu ... 1597
threshold-monitor memory ... 1599
threshold-monitor sfp ... 1601
timeout ... 1604
timeout (Telemetry) ... 1605
timers (BGP) ... 1606
timers (OSPFv2) ... 1608
timers (OSPFv3) ... 1610
topology-group ... 1612
tpvm ... 1613
traceroute ... 1616
track (VRRP) ... 1618

transport....1620
trigger....1621
trigger-function....1623
trigger-mode....1625
tvf-domain....1627
tvf-domain (interface)....1628
type....1630
uda access-list....1631
uda-key....1633
uda-key profile....1639
uda-profile-apply....1641
unlock username....1643
update-time....1644
usb....1646
usb dir....1647
usb remove....1648
use-v2-checksum....1649
user (alias configuration)....1650
username....1651
virtual-ip....1653
virtual-mac....1655
vlan....1656
vlan (EVPN)....1657
vlan dot1q tag native....1659
vrf....1660
vrf forwarding....1661
vrf mgmt-vrf....1662
vrrp-extended-group....1663
vrrp-group....1664
write erase....1666

Preface

- Conventions 27
- Documentation and Training 28
- Getting Help 28
- Providing Feedback to Us 29

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Conventions

This section discusses the conventions used in this guide.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.

Format	Description
`Courier font`	Identifies CLI output. Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	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, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

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: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. 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 and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

Subscribing to Service Notifications

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

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

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

4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Document

- Supported hardware and software....31
- What's new in this document....31

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Extreme Networks, Inc. for this SLX-OS release, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- ExtremeSwitching SLX 9140
- ExtremeSwitching SLX 9240

NOTE
Some of the commands in this document use a slot/port designation. Because the SLX 9140 and the SLX 9240 do not contain line cards, the slot designation must always be "0" (for example, 0/1 for port 1).

What's new in this document

There are new, changed, and deprecated commands in this release.

New commands

The following commands are new:

- **add destination**
- **pbf destination**
- **pbf destination-group**
- **remove destination**
- **set interface (PBF destination)**
- **show pbf destination**
- **show pbf destination-group**
- **statistics-enable**

Modified commands

The following commands are modified:

- **interface (telemetry)**
- **ip port (telemetry)**
- **profile (telemetry)**

- **set interface (NPB route-maps)**
- **show running-config telemetry profile**
- **telemetry profile**

Deprecated commands

The following commands are deprecated:

- **interface-range (telemetry)**

Using the SLX-OS CLI

- User accounts....33
- Accessing the CLI....33
- Command modes....34
- Displaying CLI commands and command syntax....35
- Completing CLI commands....36
- CLI keyboard shortcuts....36
- Using CLI command output modifiers....37
- Debug and system diagnostic commands....37
- Command shortcuts (aliases)....37

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 active management module or a Telnet or SSH session using the chassis management IP address. For more information on a serial console connection, refer to the relevant *SLX-OS Hardware Installation Guide*. For information on a session connection, refer to 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 Ethernet/IP networking administrators. You can use one of three major command modes to enter commands and access sub-configuration modes on the device.

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-0/2)# 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 0/5
device(conf-if-eth-0/5)# 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# configure terminal
device(config)# hardware
C-78(config-hardware)# ?
Possible completions:
  connector     Configure a connector
  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
  port-group    Configure a port-group
  profile       Configure Hardware Profile on a Switch
  pwd           Display current mode path
  system-mode   Set system mode
  top           Exit to top level and optionally run command
```

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

```
device# e?
Possible completions:
  end             Terminate configuration session
  event-handler   Event Handler Commands
  evpn            EVPN configuration.
  exit            Exit from current mode
```

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 l
Possible completions:
  lacp                  LACP commands
  license               Display license keys installed on the switch.
  linecard              Show linecard
  link-fault-signaling  Show Link Fault Signalling configs
  lldp                  Link Layer Discovery Protocol(LLDP).
  logging               Show logging
```

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

device# show l
Possible completions:
  lacp                  LACP commands
  license               Display license keys installed on the switch.
  linecard              Show linecard
  link-fault-signaling  Show Link Fault Signalling configs
  lldp                  Link Layer Discovery Protocol(LLDP).
  logging               Show logging
```

CLI keyboard shortcuts

The following table lists CLI keyboard shortcuts.

TABLE 1 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 2 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.
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.

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 0/2"
```

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 0/2
device(conf-if-eth-0/2)#
```

Commands A - B

aaa accounting

Configures login or command accounting; either commands or login information are forwarded to accounting servers.

Syntax

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

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

Parameters

commands
: Toggles the logging of commands.

exec
: Toggles the logging of login information.

default
: Sends the logged information to the default server.

start-stop
: Sends 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.

tacacs+
: Sends the logged information to the TACACS+ server.

none
: Disables accounting services.

Modes

Global configuration mode

Usage Guidelines

Use the **no aaa accounting** command to disable command accounting.

When logging commands, **show** commands are not forwarded.

Examples

This example configures full accounting, with the CLI information being forwarded to the TACACS+ server.

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

This example disables login accounting, but leaves command accounting active.

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

History

Release version	Command history
17s.1.00	This command was introduced.

aaa authentication

Configures the authentication, authorization, and accounting login sequence.

Syntax

aaa authentication login { **default** | **ldap** | **local** }

aaa authentication login { **radius** | **tacacs+** } { **local** | **local-auth-failback** }

no aaa authentication login

Command Default

The default server is Local.

Parameters

login

Specifies the type of server that will be used for authentication, authorization, and accounting (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 to use the local device database if prior authentication methods are inactive.

radius

Specifies the RADIUS servers.

tacacs+

Specifies the TACACS+ servers.

local

Specifies to use the local device database if prior authentication methods are inactive.

local-auth-failback

Specifies to use the local device database if prior authentication methods are not active or if authentication fails.

Modes

Global configuration mode

Usage Guidelines

This command selects the order of authentication sources to be used for user authentication during the login process. Two sources are supported: primary and secondary. The secondary source of authentication is optional and will be used if the primary source fails or is not available.

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 local-auth-fallback” to “tacacs+ local" or "tacacs+ local-auth-fallback” respectively. First remove the existing configuration and then configure it to the required configuration.

Examples

To change 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...
```

To change the AAA server from TACACS+ and local to TACACS+ only (no secondary source):

```
device# configure terminal
device(config)# aaa authentication login radius local
device(config)# do show running-config aaa
aaa authentication login radius
device(config)# aaa authentication login tacacs+
device(config)# do show running-config aaa
aaa authentication login tacacs+
```

History

Release version	Command history
17s.1.00	This command was introduced.

action

Specifies which classification type in the policer remarking profile is being modified and whether the classification type applies to conforming traffic or exceeding traffic.

Syntax

action *classification-type* **conform** | **exceed**

Command Default

The **police-remark-profile** command has been executed.

Parameters

classification-type

Specifies the classification type to be modified in the default policier remarking profile. Choices include:

- color
- color-and-cos
- color-and-dscp
- color-and-traffic-class

conform

Specifies that the settings for the classification type apply to conforming traffic.

exceed

Specifies that the settings for the classification type apply to exceeding traffic.

Modes

Policer remarking profile configuration mode

Usage Guidelines

Use this command after executing the **police-remark-profile** command. If you specify "color" as the choice for *classification-type*, then you issue the **set** command to specify parameters for cos, traffic-class, and dscp. If you specify any of the other choices for *classification-type*, then you issue the **map** command to include the parameters in the specified map in the default policer remark profile.

Examples

The following is an example of executing the **action** command to specify the color classification type for conforming traffic. Then, the example shows using the **set** command to specify the settings for the remark values in the default policer remark profile.

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color conform
device(police-remark-profile-color-conform)# set cos 3
device(police-remark-profile-color-conform)# set traffic-class 5
device(police-remark-profile-color-conform)# set dscp 10
device(police-remark-profile-color-conform)# exit
```

The following is an example of executing the **action** command to specify the color-and-cos classification type for exceeding traffic. Then, the example shows using the **map** command to specify the maps to be included in the default policer remark profile for cos remarking for exceeding traffic. ("cm1," "ct1," and "cd1" are map names).

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color-and-cos exceed
device(police-remark-profile-color-and-cos-exceed)# map cos-mutation cm1
device(police-remark-profile-color-and-cos-exceed)# map cos-traffic-class ct1
device(police-remark-profile-color-and-cos-exceed)# map cos-dscp cd1
device(police-remark-profile-color-and-cos-exceed)# exit
```

The following is an example of executing the **action** command to specify the color-and-dscp classification type for conforming traffic. Then, the example shows using the **map** command to specify the maps to be included in the default policer remark profile for dscp remarking for conforming traffic. ("dm1," "dc1," and "dt1" are map names).

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color-and-dscp conform
device(police-remark-profile-color-and-dscp-conform)# map dscp-mutation dm1
device(police-remark-profile-color-and-dscp-conform)# map dscp-cos dc1
device(police-remark-profile-color-and-dscp-conform)# map dscp-traffic-class dt1
device(police-remark-profile-color-and-dscp-conform)# exit
```

The following is an example of executing the **action** command to specify the color-and-traffic-class classification type for exceeding traffic. Then, the example shows using the **map** command to specify the maps to be included in the default policer remark profile for traffic-class remarking for exceeding traffic. ("tm2," "tc2," and "td2" are map names).

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color-and-traffic-class exceed
device(police-remark-profile-color-and-traffic-class-exceed)# map traffic-class-mutation tm2
device(police-remark-profile-color-and-traffic-class-exceed)# map traffic-class-cos tc2
device(police-remark-profile-color-and-traffic-class-exceed)# map traffic-class-dscp td2
device(police-remark-profile-color-and-traffic-class-exceed)# exit
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

action-timeout

Specifies the maximum number of minutes to wait for an action-script to complete execution.

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

If the action-timeout expires, then script execution ends.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 streaming 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 collector_1
device(config-collector-collector_1)# activate
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

activate (VXLAN gateway)

Activates a VXLAN overlay gateway instance.

Syntax

activate

no activate

Command Default

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

Modes

VXLAN 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 both the nodes of the logical VTEP (LVTEP),
- All loopback interfaces must be configured with the same IPv4 address and the same VRF instance.
- 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" when the gateway is previously configured by means of the **overlay-gateway** command.

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

History

Release version	Command history
17s.1.01	This command was introduced.

add (telemetry)

Restores a previously removed field to a telemetry profile.

Syntax

add *telemetry-field*

no add *telemetry-field*

Command Default

All of the default fields are included in the telemetry profile.

Parameters

telemetry-field

Specifies the profile field.

Modes

Telemetry-profile configuration mode

Usage Guidelines

To remove a field from a profile, use the **no** form of this command.

Examples

The following example removes the **buffers** field from the **default_system_utilization_statistics** profile.

```
device# configure terminal
device(config)# telemetry profile system-utilization default_system_utilization_statistics
device(config-system-utilization-default_system_utilization_statistics)# no add buffers
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.00	Additional enhanced statistic fields added.

add destination

Adds policy-based forwarding (PBF)-destinations to a destination group.

Syntax

add destination *destination-id*

no add destination

Command Default

PBF destination groups contains no PBF destinations.

Parameters

destination-id

Specifies one or more PBF destination IDs. You can specify one ID, a range (example: 3-5), a comma-separated list (example: 1,3,5,6), or combine IDs, ranges, and lists (example: 1-5,6,8).

Modes

PBF destination-group configuration mode

Usage Guidelines

The use case for this command is under Network Packet Broker (NPB) system mode.

To remove all PBF destination IDs included in a destination group, use the **no add destination** form of this command.

To remove some of the PBF destination IDs included in a destination group, use the **remove destination** *destination-id* command.

Examples

The following example creates a PBF destination-group and adds three PBF destinations to it.

```
device# configure terminal
device(config)# pbf destination-group 171
device(config-destination-group-171)# add destination 10,20,30
```

The following example accesses the above PBF destination-group and removes all PBF destinations from it.

```
device# configure terminal
device(config)# pbf destination-group 171
device(config-destination-group-171)# no add destination
```

History

Release version	Command history
18s.1.02	This command was introduced.

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

This feature is 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)#
```

History

Release version	Command history
17s.1.01	This command was introduced.

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*]

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

The **no** form of the command removes 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)#
```

The following 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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command Default

Advertisement is disabled.

Modes

Protocol LLDP configuration mode

Profile configuration mode

Examples

The following example advertises TLV configuration for IEEE 802.1.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command Default

Advertisement is disabled.

Modes

Protocol LLDP configuration mode

Profile configuration mode

Examples

The following example advertises TLV configuration for IEEE 802.3.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

If a backup router is enabled to send advertisement frames, the frames are sent every 60 seconds.

This command can be used for VRRP-E, but not for VRRP.

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

Examples

To enable 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 configuration mode

Profile configuration mode

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 management-address port-description
```

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

```
device(conf-lldp)# profile test1
device(conf-profile-test1)# advertise optional-tlv management-address
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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 100 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

advertisement-interval-scale

Configures subsecond 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 set to 1 second and the scaling value is set to 10, the new advertisement interval is 100 milliseconds. When all the advertisement intervals in a VRRP-Ev3 session are scaled, subsecond 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 subsecond advertising intervals, subsecond device redundancy can be achieved.

This command is only supported by VRRP-Ev3.

Examples

To set 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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

The **no** form of the command disables this feature so that the device advertises individual routes for all networks.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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"
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

allow-vn-tag

Changes an interface from the default support for 802.1BR headers to support for VN-Tag headers.

Syntax

allow-vn-tag

no allow-vn-tag

Command Default

802.1BR headers are supported and VN-Tag headers are not supported.

Modes

Interface configuration mode

Usage Guidelines

To learn where default support for 802.1BR headers was changed to support for VN-Tag headers—by running **allow-vn-tag**—run the **show running-config interface** command:

- VN-Tag interfaces display `allow-vn-tag`.
- 802.1BR interfaces do not display `allow-vn-tag`.

This command is supported only under network packet-broker (NPB) system-mode.

Disabling 802.1BR header-mode on an interface also disables E-Tag support on that interface.

After you run this command, you do not need to reboot SLX-OS.

The **no** form of this command disables support for VN-Tag headers and restores the default support for 802.1BR headers.

Examples

The following example enables VN-Tag header-mode on an interface, disabling the default 802.1BR mode.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(config-if-eth-0/1)# allow-vn-tag
```

The following example restores the default 802.1BR header-mode on an interface, disabling support for VN-Tag headers.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(config-if-eth-0/1)# no allow-vn-tag
```

History

Release version	Command history
18s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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 so that the device does not advertise BGP routes not installed in the RIB manager.

Examples

The following 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
```

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

announce-interval

Configures the interval at which a Precision Time Protocol (PTP) slave clock receives PTP Announce messages from a master clock.

Syntax

announce-interval [*interval*]

no announce-interval

Command Default

The default Announce message interval is 0 log seconds.

Parameters

interval

PTP Announce interval, in log seconds. Range is from 0 through 4. The default is 0 (1 packet/second).

Modes

PTP configuration mode

Interface subtype configuration mode

Usage Guidelines

This interval is configured on the interface of a slave device. The value for *interval* must be consistent on all Extreme SLX-OS devices within a single PTP domain.

The inputs for *interval* represent base 2 exponents, where the packet rate is $1/(2^{\log \text{seconds}})$.

Use the **no** form of this command to revert to the default interval.

Examples

To configure a PTP Announce interval of 2 packets per second 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)# announce-interval 1
```

To revert to the default interval:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# protocol ptp
device(conf-if-eth-0/1)# no announce-interval
```

History

Release version	Command history
17s.1.00	This command was introduced.

announce-timeout

Configures the number of Announce message intervals that elapse before a timeout occurs on an interface.

Syntax

announce-timeout *count*

no announce-timeout

Command Default

Default number of Announce message intervals before a timeout is 3.

Parameters

count

Number of Announce message intervals. Range is from 3 through 10. The default is 3.

Modes

PTP configuration mode

Interface subtype configuration mode

Usage Guidelines

The value for *count* must be consistent on all Extreme SLX-OS devices within a single PTP domain.

Use the **no** form of this command to revert to the default Announce message interval of 3.

Examples

To configure a PTP Announce timeout interval of 9 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)# announce-timeout 9
```

To revert to the default PTP Announce timeout interval of 3:

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# protocol ptp
device(conf-if-eth-0/2-ptp)# no announce-timeout
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Valid values rante from 1 through 16777215.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 *num*
Specifies the OSPF route metric.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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

OSPF router configuration mode

OSPF 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 10.1.1.0 10.255.255.0 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 10.255.255.0 advertise
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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.

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

area stub (OSPFv2)

Creates or deletes a stub area or modifies its parameters.

Syntax

area { *A.B.C.D* | *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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

arp

Creates a static Address Resolution Protocol (ARP) entry.

Syntax

arp *A.B.C.D mac-address* **interface** { **ethernet** *slot* **/** *port* | **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. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

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 0/1
```

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 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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.

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 implements DAI:

1. Creates an ARP ACL named "arp_acl_1".
2. Defines **permit ip host** rules in that ACL.
3. Applies the ACL to VLAN 200.
4. Enables dynamic ARP inspection (DAI) on VLAN 200.

```
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 range is from 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 to use for RADIUS server 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

auto-cost reference-bandwidth (OSPFv2)

Configures reference bandwidth.

Syntax

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

no auto-cost reference-bandwidth

Parameters

value

Reference bandwidth in Mbps. Valid values range from 1 through 4294967. The default reference bandwidth is 100 Mbps.

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 combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

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.

History

Release version	Command history
17s.1.00	This command was introduced.

auto-cost reference-bandwidth (OSPFv3)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth *value*

no auto-cost reference-bandwidth

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 combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

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.

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The banner can appear on multiple lines if you enter multiline mode by using **Esc-M** and exit by using **CTRL-D**.

Use the **no** form of the command to delete the banner.

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"
```

History

Release version	Command history
17s.1.00	This command was introduced.

basedn

Defines the base domain name of the LDAP host.

Syntax

basedn { *basedn* }

no basedn

Command Default

The base domain name is not defined.

Parameters

basedn

The base domain name of the LDAP host.

Modes

LDAP host configuration mode.

Usage Guidelines

Use the **no** form of this command to remove the base domain name.

Examples

To change the domain in an existing configuration:

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# basedn security.extreme.com
```

Executing **no** on an attribute sets it with its default value.

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# no basedn
```

History

Release version	Command history
17s.1.00	This command was introduced.

bfd

Enables Bidirectional Forwarding Detection (BFD).

Syntax

bfd

no bfd

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

VXLAN overlay gateway site configuration mode

Usage Guidelines

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.

Use the **bfd** command in VXLAN overlay gateway site configuration mode to configure BFD for Layer 2 extension tunnels. Use the **no** form of this command in VXLAN overlay gateway site configuration mode to disable BFD for the tunnel.

The **no** form of the command disables BFD globally in OSPF router configuration mode or OSPFv3 router configuration mode.

Examples

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
```

The following example enables BFD globally in a nondefault VRF instance.

```
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ipv6-router-ospf-vrf-red)# bfd
```

The following example enables BFD on a VXLAN overlay gateway site.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site s1
device(config-site-s1)# bfd
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	Support was added for VXLAN overlay gateway site configuration mode.

bfd holdover-interval

Sets the time interval for which Open Shortest Path First (OSPF) 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*

Parameters

time

Specifies the BFD holdover interval in seconds. In BGP configuration mode, valid values range from 1 through 30 and the default is 0. In OSPF router VRF and OSPFv3 router VRF configuration mode, valid values range from 1 through 20, and the default is 0.

Modes

BGP 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.

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 to 20 for VRF instance “red” in OSPFv3 router VRF configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ipv6-router-ospf-vrf-red)# bfd holdover-interval 20
```

History

Release version	Command history
17s.1.00	This command was introduced.

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, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000. The default is 200 for chassis platforms. The default is 500 for non-chassis platforms. In VXLAN overlay gateway site configuration mode, valid values range from 100 through 30000, and the default is 100 on all platforms.

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 200 for chassis platforms. The default is 500 for non-chassis platforms. In VXLAN overlay gateway site configuration mode, valid values range from 300 through 30000, and the default is 300 on all platforms.

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

VXLAN overlay gateway site 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 will be the negotiated values.

Use the **bfd interval** command in BGP configuration mode for multihop sessions only. Single-hop sessions in BGP use either the values configured at the interface level using the **bfd interval** command or the default interval values.

The **no** form of the command reverts to the default parameters.

Examples

The following example sets the BFD session parameters globally 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 globally 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
```

The following example sets the BFD session parameters on a VXLAN overlay gateway site.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site s1
device(config-site-s1)# bfd interval 2000 min-rx 3000 multiplier 26
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	Support was added for VXLAN overlay gateway site configuration mode.

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.

Examples

The following example disables BFD sessions on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# bfd shutdown
```

The following example disables BFD sessions on a specific virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-Ve-24)# bfd shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

bgp-redistribute-internal

Causes the device to allow the redistribution of iBGP routes from BGP into OSPF.

Syntax

bgp-redistribute-internal

no bgp-redistribute-internal

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, 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, by default the device allows the redistribution of iBGP routes from BGP into OSPF.

The **no** form of the command disables BGP route redistribution.

Examples

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

breakout mode

Configures 40-Gbe or 100-Gbe ports as four 10-Gbe or four 25-Gbe ports dynamically.

Syntax

breakout mode { **4x10g** | **4x25g** }

no breakout

Command Default

See the Usage Guidelines.

Parameters

4x10g

Specifies 4x10G mode.

4x25g

Specifies 4x25G mode.

Modes

Hardware connector configuration mode

Usage Guidelines

Dynamic breakout is supported; the user does not need to reboot the switch to execute the breakout.

Examples

The following example shows the steps to configure 4x10G breakout mode on a 40G/100G port.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# connector 0/49
device(config-connector-0/49)# breakout mode 4x10g
%Warning: Sfp Breakout is a disruptive command.
device(config-port-group-0/49)# Ctrl-z
device# copy running-config startup-config
This operation will modify your startup configuration.
Do you want to continue? [y/n]: y
device#
```

The following examples confirm the configuration.

```
device(config-connector-0/49)# do show ip interface brief | include
49
Ethernet 0/49          unassigned           default-vrf             administratively down
down

SLX(config-connector-0/49)# breakout mode 4x25g
SLX(config-connector-0/49)# do show ip interface brief | include
49
Ethernet 0/49:1        unassigned           default-vrf             administratively down     down
Ethernet 0/49:2        unassigned           default-vrf             administratively down     down
Ethernet 0/49:3        unassigned           default-vrf             administratively down     down
Ethernet 0/49:4        unassigned           default-vrf             administratively down     down
SLX(config-connector-0/49)# no breakout
SLX(config-connector-0/49)# do show ip interface brief | include
49
Ethernet 0/49          unassigned           default-vrf             administratively down     down
SLX(config-connector-0/49)#
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.01	Support for dynamic dual breakout mode was added.

bridge-domain

Creates a bridge domain.

Syntax

bridge-domain { *id* } [**p2mp** | **p2p**]

no bridge-domain { *id* } [**p2mp** | **p2p**]

Command Default

No bridge domain is configured.

Parameters

id

Specifies a unique numeric bridge-domain identifier. On SLX 9140, the range is from 1 through 4096. On SLX 9240, the range is from 1 through 3566.

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 SLX device supports bridge domain on an MCT cluster.

The **no** version of the 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

bridge-domain (EVPN)

Configures a bridge domain (BD) in Ethernet VPN (EVPN) instance configuration mode and enters EVPN bridge-domain configuration mode.

Syntax

bridge-domain *number* [**add** | **remove**]

no bridge-domain *number*

Command Default

No bridge domain is configured.

Parameters

number

Specifies an EVPN bridge domain. On SLX 9140, the range is from 1 through 4096. On SLX 9240, the range is from 1 through 3566.

add

Adds a bridge domain or range of bridge domains to the EVPN instance.

remove

Removes a bridge domain or range of bridge domains from the EVPN instance.

Modes

EVPN instance configuration mode

Usage Guidelines

Use the **no** form of this command to delete a bridge domain from an EVPN instance.

Examples

To specify a bridge domain for an EVPN instance and enter EVPN bridge-domain configuration mode:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# bridge-domain 1
device(evpn-bridge-domain-1)#
```

To add a bridge domain to the EVPN instance:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# bridge-domain add 10
```

To remove a range of bridge domains from the EVPN instance:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# bridge-domain remove 10-20
```

To delete a bridge domain from the EVPN instance:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# no bridge-domain 10
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

bsr-candidate

Configures a bootstrap router (BSR) as a candidate to distribute rendezvous point (RP) information to the other PIM Sparse devices within a PIM Sparse domain.

Syntax

bsr-candidate interface [*ethernet* | *loopback* | *port-channel*| *ve*]

no bsr-candidate

Command Default

The PIM router does not participate in BSR election.

Parameters

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.

Modes

PIM Router configuration mode

Usage Guidelines

The **no** form of this command makes the PIM router cease to act as a candidate BSR.

Each PIM Sparse domain has one active BSR. For redundancy, you can configure ports on multiple devices as candidate BSRs. The PIM Sparse protocol 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, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

Examples

The following example uses a physical interface to configure a device as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate ethernet 2/2 30 255
```

The following example uses a loopback interface to configure a device as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate interface loopback 11 mask 32
```

The following example uses a virtual interface to configure a device as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate ve 120 30 250
```

History

Release version	Command history
17s.1.00	This command was introduced.

Commands C - D

capability as4-enable

Enables 4-byte autonomous system number (ASN) capability at the BGP global level.

Syntax

capability as4-enable

no capability as4-enable

Command Default

4-byte ASN capability is disabled.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command disables 4-byte ASN capability if it has been enabled.

Examples

The following example enables 4-byte ASN capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# capability as4-enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

capture packet interface ethernet

Captures frames ingressing or egressing an Ethernet port.

Syntax

capture packet interface ethernet *slot***/** *port*

capture packet interface ethernet *slot* **/** *port* **direction** { **both** | **rx** | **tx** } **filter** { l2 | l3 }

capture packet interface ethernet *slot* **/** *port* **direction** { **both** | **rx** | **tx** } **filter all** [**packet-count** *count*]

no capture packet interface ethernet *slot* **/** *port*

Command Default

The capture packet interface Ethernet feature is disabled.

Parameters

slot

Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port

Specifies a valid port number.

direction

Specifies the direction of the frames.

both

(Not currently supported) Specifies frames either ingressing or egressing out through the port.

rx

Specifies frames ingressing into the port.

tx

Specifes frames egressing through the port.

filter

Specifies the filter.

l2

Captures only L2 control frames.

l3

Captures only L3 control frames.

all

Captures all supported frames on the port, as described in the Guidelines.

packet-count *count*

(Supported only in NPB system-mode, for the **all** option) Specifies the number of frames. The valid range is from 1 through 8000. The default is 2048.

Modes

Privileged EXEC mode

Usage Guidelines

In default system-mode, control frames and ACL-logged frames are captured.

In Network Packet Broker (NPB) system-mode, data frames are also captured.

When packet capture is active, the frames are saved to `/tmp/pktcapture_running.pcap`. Upon termination of packet capture (at **packet-count** *count* or by running **no capture packet interface ethernet**, this file is renamed `/tmp/pktcapture.pcap`. By using the Unix **scp** command, you can securely copy`/tmp/pktcapture.pcap` for analysis.

Examples

(Under NPB system-mode) The following example captures up to 5000 frames ingressing to an Ethernet interface.

```
device# capture packet interface ethernet 0/9 direction rx filter all packet-count 5000
```

History

Release version	Command history
18s.1.01	This command was introduced.

cee

Applies the configured CEE map to the interface. This command also activates and configures QoS flow control on the interface.

Syntax

cee default

no cee

Modes

Interface subtype configuration mode

Usage Guidelines

The only map name allowed is named default.

Use the **no** form of this command to remove the CEE map from the interface.

Examples

The following example configures the default CEE map to the interface.

```
device# configure terminal
device(config)# interface Ethernet 0/6
device(conf-if-eth-0/6)# cee default
```

History

Release version	Command history
17s.1.00	This command was introduced.

cee-map default

Accesses the default CEE map configuration mode.

Syntax

cee-map default

Modes

Global configuration mode

Usage Guidelines

The only map name allowed is named default.

Examples

The following example accesses the default CEE map configuration mode.

```
device# configure terminal
device(config)# cee-map default
device(config-cee-map-default)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

certutil import sshkey

Imports the SSH public key for an SSH user from the remote host using the mentioned login credentials and path name.

Syntax

certutil import sshkey host *remote_ip_address* **directory** *ssh_public_key_path* **file** *filename* **user** *user_acct* **password** *password* **login** *login_id*

no certutil sshkey

Parameters

host *remote_ip*
Specifies the IP address of the remote host.

directory *path*
Specifies the path to the certificate.

file *filename*
Specifies the SSH public key with a .pub extension.

user *user_acct*
Specifies the user name to access the remote host.

password *password*
Specifies the password to access the remote host.

login *login_id*
Specifies the login name in the remote host.

file *filename*
Specifies the SSH public key with a .pub extension.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **no certutil sshkey user** to delete the SSH public key a specified user.

When using the 'pass' parameter with special characters (such as #$@`) use single or double-quotes around the password. Alternatively, the special characters can be escaped with a backslash (\) preceding the special character.

Examples

The following command deletes the SSH public key for "testuser."

```
device# no certutil sshkey user testuser
 Do you want to delete the SSH public key file? [y/n]:y
device# 2012/11/11-13:46:05, [SEC-3050], 3295,, INFO, Event: sshutil, Status: success, Info: Deleted
SSH public keys associated to user 'testuser'.
```

The following command deletes the SSH public key for "testuser."

```
device# no certutil sshkey user testuser
 Do you want to delete the SSH public key file? [y/n]:y
device# 2012/11/11-13:46:05, [SEC-3050], 3295,, INFO, Event: sshutil, Status: success, Info: Deleted
SSH public keys associated to user 'testuser'.
```

The following commands demonstrate 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\!
device# certutil import ssh host 192.168.10.10 dir /home/brcd1/.ssh file id_rsa.pub user admin login
brcd1 pass "Abcde!"
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 a Link Aggregation Group (LAG) port-channel group number to which this link should administratively belong. Values range from 1 through 6144.

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

This command adds an interface to a port-channel specified by the channel-group number. This command enables link aggregation on an interface, so that it may be selected for aggregation by the local system.

The maximum number of LAGs supported is 24.

A maximum of 16 links can be aggregated per port-channel.

To remove port-channel members, use the **no** form of this command.

Examples

The following example sets the channel-group ID to 10 and the mode to "passive".

```
device# configure terminal
device(config)# interface ethernet 0/9
device(conf-if-eth-0/9)# channel-group 10 mode passive
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.02c, 18s.1.00	This command was modified, ending support for the "brocade" channel-group type.

chassis

Sets the IPv4 or IPv6 address of a device chassis.

Syntax

chassis { **virtual-ip** *IPv4-address* | **virtual-ipv6** *IPv6-address* }

no chassis

Command Default

The default is the initial address of the device chassis.

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 default chassis IPv4 or IPv6 address. The default is the initial address of the device chassis.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

chassis fan airflow-direction

Specifies the direction of airflow through the chassis based on physical PSU and fans.

Syntax

chassis fan airflow-direction [**port-side-intake** | **port-side-exhaust**]

Parameters

port-side-intake
Specifies the airflow to enter the switch.

port-side-exhaust
Specifies the airflow to exit the switch.

Modes

Privileged EXEC mode

Usage Guidelines

This command must only be used after you purchase and install the appropriate fan/power supply that provides the desired airflow direction in the switch. Please contact your Sales Representative to obtain the correct part numbers and pricing.

When the **chassis fan airflow-direction** command is issued, the switch will not recognize the configuration change until the switch is rebooted.

Only one (1) configuration change is accepted per reboot. This means that even if this command is entered multiple times, only the first configuration change entered will be effective after rebooting.

The switch serial number is registered with Extreme and the information recorded in the Extreme database about that switch includes the airflow orientation at the time of shipment. Any subsequent change in airflow direction is not recorded in the Extreme database. This means that if you request a Return Merchandise Authentication (RMA) for the switch, the replacement switch will be sent with the original orientation.

Examples

To specify the fan airflow-direction:

```
device# chassis fan airflow-direction port-side-exhaust

Previous configuration : port-side-intake
Current configuration  : port-side-exhaust
System fan airflow-direction changes will be effective after reboot!!
```

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 has been created. Two classes, "default" and "cee", cannot be created or deleted.

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 have been created and associated with match criteria using the **class-map** command. (Refer to the **qos cos** command.) When you launch the **class** command while in policy map configuration mode (refer to **policy-map**) for a policy, the system is placed in "configure policy-map classification" (config-policymap-class) mode.

Each policy map can contain one class map. The **police cir** command is mandatory for configuring a class map.

Enter the **no class** *class-mapname* command to remove the class from the policy map.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 names "default" and "cee" are 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.

You can create up to 128 class maps.

Examples

To create a class map and place system into config-classmap mode:

```
device(config)# class-map default
device(config-classmap)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Must be `0` if the switch does not contain slots.

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.

Examples

The following example clears all ARP entries on the device.

```
device# clear arp
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear bgp evpn neighbor

Clears specified or all EVPN neighbors.

Syntax

clear bgp evpn neighbor { *IPv4-address* | *IPv6-address* | **all** } [**soft** { **in** | **out** } | **soft-outbound**]

Command Default

EVPN neighbors are not cleared.

Parameters

IPV4-address
Specifies an IPv4 address.

IPV6-address
Specifies an IPv6 address.

all
Specifies all addresses.

soft
Sends a route refresh or resends routes to the specified neighbor from the RIB-out table.

in
Sends a route refresh.

out
Resends routes to the specified neighbor from the RIB-out table.

soft-outbound

Modes

Privileged EXEC mode

Examples

To clear all IPv4 EVPN neighbors and send a route refresh:

```
device# clear bgp evpn neighbbor 10.10.10.0 all soft in
```

History

Release version	Command history
17s.1.01	This command was introduced.

clear bgp evpn routes

Clears all or specified EVPN routes in the EVPN routing table, and triggers running import rules on the routes received.

Syntax

clear bgp evpn routes { *IPv4-address* | *IPv6-address* | **all** }

Command Default

EVPN neighbors are not cleared.

Parameters

IPV4-address
Specifies an IPv4 address.

IPV6-address
Specifies an IPv6 address.

all
Specifies all addresses.

Modes

Privileged EXEC mode

Examples

To clear IPv4 EVPN routes and trigger running import rules on the routes received:

```
device# clear bgp evpn routes 10.10.10.0
```

History

Release version	Command history
17s.1.01	This command was introduced.

clear bgp evpn routes type

Clears the BGP EVPN IGMP Join or Leave Sync routes from the EVPN routing table.

Syntax

clear bgp evpn routes type igmp-join-sync|igmp-leave-sync

Parameters

igmp-join-sync
Clears the IGMP Join Sync routes from the EVPN routing table.

igmp-leave-sync
Clears the IGMP Leave Sync routes from the EVPN routing table.

Modes

Privileged EXEC mode

Examples

The following example clears the IGMP Join Sync routes from the EVPN routing table.

```
device# clear bgp evpn routes type igmp-join-sync
```

History

Release version	Command history
18s.1.01	This command was introduced.

clear counters

Clears the IP counter statistics on the device.

Syntax

clear counters all |[**interface** { { **ethernet***0/port* | **fibrechannel** *0/port* | **port-channel** *number* | **vlan** *vlan_id* }] **slot***0*]

Parameters

all

Clears all IP counter statistics on the device or selected interface.

interface

Specifies an interface.

ethernet

Specifies a physical Ethernet interface.

0

Specifies a valid slot number. The only valid slot number is 0.

port

Specifies a valid port number.

fibrechannel

Specifies a fibrechannel interface.

0

Specifies a valid slot number. The only valid slot number is 0.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel. The number of available channels range from 1 through 6144.

slot *0*

Specifies a valid slot id. The only valid slot number is 0.

Modes

Privileged EXEC mode

Examples

The following example clears all counter statistics.

```
device# clear counters access-list interface ethernet 2/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear counters access-list

For a given network protocol and inbound/outbound direction, clears ACL statistical information. 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 interface, VLAN, or VE.

Syntax

clear counters access-list interface { **ethernet** *0* **/** *port* | **port-channel** *index* | **vlan** *vlan_id* } { **in** | **out** }

clear counters access-list interface ve *vlan_id* { **in** | **out** }

clear counters access-list { **ip** | **ipv6** | **mac** } [*acl-name* { **in** | **out** }]

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* { **global in** }]

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.

0
Specifies a valid slot number. The only valid slot number is 0.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel. Available channels range from 1 through 6144.

in | **out**
Specifies the binding direction (incoming or outgoing).

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 | **ipv6** | **mac**
Specifies the network protocol.

global
Specifies Level 3 receive ACLs (rACLs), which are applied at device-level, rather than at interface-level.

mac *acl-name*
Specifies the MAC ACL name. To clear statistics on all counters of an ACL-type, do not specify *acl-name*.

in | **out**
Specifies the binding direction (incoming or outgoing).

Modes

Privileged EXEC mode

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 receive-path ACL statistics for a specified IPv6 ACL.

```
device# clear counters access-list ipv6 ipv6_acl_10 global in
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear counters link-fault-signaling

Clears link-fault signaling (LFS) counter information for all interfaces or for a specified interface.

Syntax

clear counters link-fault-signaling [**all**]

clear counters link-fault-signaling slot *slot-num*

clear counters link-fault-signaling interface ethernet *slot* **/** *port* { **all** | **local** | **remote** }

Parameters

all
Specifies local and remote LFS counters on all interfaces.

slot *slot-num*
Specifies a valid slot number. Must be `0` if the device does not contain slots.

interface ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the device does not contain slots.

port
Specifies a valid port number.

all
Specifies local and remote LFS counters.

local
Specifies local LFS counters only.

remote
Specifies remote LFS counters only.

Modes

Privileged EXEC mode

Examples

The following example clears local and remote LFS counters on all interfaces.

```
device# clear counters link-fault-signaling all
```

The following example clears local LFS counters on a specified interface.

```
device# clear counters link-fault-signaling interface ethernet 0/2 local
```

History

Release version	Command history
17s.1.02	This command was introduced.

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 0/***port*]

clear counters storm-control interface ethernet 0/*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 0/*port*
Clears all BUM-related counters in the system for the specified interface.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear dot1x statistics

Clears accumulated dot1x port authentication statistics on a port.

Syntax

clear dot1x statistics [**interface ethernet** *slot/port*]

Parameters

interface ethernet *slot/port*

Causes clearing of all dot1x statistics for a specified interface port. When the switch does not contain slots, the slot number must be 0.

Modes

Privileged EXEC mode

Examples

The following example clears accumulated dot1x port authentication statistics on all ports.

```
device# clear dot1x statistics
```

The following example clears all dot1x statistics for a specific Ethernet port (0/1).

```
device# clear dot1x statistics interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. On SLX 9140, the range is from 1 through 4096. On SLX 9240, the range is from 1 through 3566.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ip arp suppression-statistics

Clears ARP-suppression statistical information. 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. On SLX 9140, the range is from 1 through 4096. On SLX 9240, the range is from 1 through 3566.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
: IPv4 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 ip bgp dampening
```

The following example unsuppresses suppressed BGP4 routes for VRF "red".

```
device# clear ip bgp dampening vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
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

The following example clears the dampening statistics for a BGP4 route.

```
device# clear ip bgp flap-statistics 10.0.0.0/16
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example clears all BGP4 local routes.

```
device# clear ip bgp local routes
```

The following example clears BGP4 local routes for VRF "red".

```
device# clear ip bgp local routes vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

ip-addr
Clears all BGP4 connections with this IPv4 address, in dotted-decimal notation.

peer-group-name
Clears all BGP4 connections in this peer group. Range is from 1 through 63 characters.

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

The following example refreshes all BGP4 neighbor connections.

```
device# clear ip bgp neighbor all
```

The following example refreshes all BGP4 neighbor connections for VRF "red".

```
device# clear ip bgp neighbor all vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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

The following example clears all BGP4 routes.

```
device# clear ip bgp routes 10.0.0.0/16
```

The following example clears BGP4 routes for VRF instance "red":

```
device# clear ip bgp routes 10.0.0.0/16 vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ip igmp groups

Clears information related to learned groups in the IGMP module.

Syntax

clear ip igmp groups [**vlan** *vlan-id* | {**cluster** [*id*] }| **client** *client-id* }]

Parameters

vlan*vlan-id*

Specifies a VLAN.

cluster [*id*]

Specifies the cluster or optionally the cluster ID to clear all groups learned through MCT on the MCT cluster.

client *id*

Specifies the cluster client ID to clear all groups learned on the Cluster Client Edge Port (CCEP).

Modes

Privileged EXEC mode

Examples

To clear information for all groups in the IGMP protocol:

```
device# clear ip igmp groups
```

To clear information for all IGMP routes learned over the MCT cluster:

```
device# clear ip igmp groups cluster 1
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.01	Added the cluster, cluster ID, and client ID options.

clear ip igmp statistics

Clears statistical information related to the IGMP database.

Syntax

clear ip igmp statistics [**vlan** *vlan-id*]

Parameters

vlan*vlan-id*

Specifies a VLAN.

Modes

Privileged EXEC mode

Examples

The following example clears statistics information for a VLAN in the IGMP protocol.

```
device# clear ip igmp statistics vlan 11
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ip ospf

Clears OSPF data processes, counters, neighbors, or routes.

Syntax

clear ip ospf all [**vrf** *vrf-name*]

clear ip ospf counters { **all** | **ethernet** *slot/port* | **loopback** *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 *vrf-name*
Specifies a VRF.

counters
Clears OSPF counters.

all
Clears all counters.

ethernet *slot* **/** *port*
Specifies an Ethernet slot and port. The slot number must be 0 if the switch does not contain slots.

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.

neighbor
Clears specified 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 the OSPF processes.

```
device# clear ip ospf all
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ip route

Clears a specified route or all IP routes in the IP routing tables.

Syntax

clear ip route { **all** | [**slot 0** [**vrf** *vrf-name*]] }

clear ip route slot 0

Parameters

all

Removes all IPv4 routes.

vrf *vrf-name*

Removes IPv4 routes for the specified VPN Routing and Forwarding (VRF) instance.

slot *0*

Removes Clear IP route on slot ID (LP only) . The only valid slot number is 0.

Modes

Privileged EXEC mode

Examples

The following example clears the IP route specified by IP address 192.158.1.0/24.

```
device# clear ip route 192.158.1.0/24
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ipv6 bgp flap-statistics

Clears route-flap statistics for BGP4+ routes.

Syntax

clear ipv6 bgp flap-statistics [*ipv6-addr* { **/** *mask* } | **neighbor** *ipv6-addr* | **regular-expression** *string*] [**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.

neighbor
Clears route-flap statistics only for routes learned from the specified neighbor.

ipv6-addr
IPv6 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

The following example clears all dampening statistics for a BGP4+ route.

```
device# clear ipv6 bgp flap-statistics
```

The following example clears the dampening statistics for a BGP4+ route for VRF "red".

```
device# clear ipv6 bgp flap-statistics vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example clears all BGP4+ local routes.

```
device# clear ipv6 bgp local routes
```

The following example clears BGP4+ local routes for VRF "red".

```
device# clear ipv6 bgp local routes vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example refreshes all BGP4+ neighbor connections.

```
device# clear ipv6 bgp neighbor all
```

The following example resets all the counters for BGP4+ messages.

```
device# clear ipv6 bgp neighbor all traffic
```

The following example clears BGP4+ connections with a specified peer group.

```
device# clear ipv6 bgp neighbor P1
```

The following example clears BGP4+ connections with a specified peer group for VRF "red".

```
device# clear ipv6 bgp neighbor P1 vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
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 clears specific BGP4+ routes.

```
device# clear ipv6 bgp routes 2000::/64
```

The following example clears specific BGP4+ routes for VRF "red".

```
device# clear ipv6 bgp routes 2000::/64 vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example clears all BGP4+ message counters.

```
device# clear ipv6 bgp traffic
```

The following example clears BGP4+ message counters for VRF "red".

```
device# clear ipv6 bgp traffic vrf red
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **ve** *ve-id* }

Parameters

all

Specifies all interfaces.

interface

Specifies interface.

ethernet

Represents a valid, physical Ethernet subtype.

slot

Specifies a valid slot number as 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.

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 interface 0/1.

```
device# clear ipv6 counters interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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-address*

IPv6 address of DHCP server where client requests are to be forwarded.

Modes

Privileged EXEC mode

Examples

Clear all the DHCP Relay statistics on the device.

```
device# clear ipv6 dhcp relay statistics
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ipv6 mld groups

Clears IPv6 MLDv1 group cache entries for a VLAN.

Syntax

clear ipv6 mld groups vlan *vlan-id*

Parameters

vlan*vlan-id*

Specifies the VLAN ID.

Modes

Privileged EXEC mode

Examples

To clear IPv6 MLDv1 groups for a specific VLAN:

```
device# clear ipv6 mld groups vlan 1
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ipv6 mld statistics

Clears IPv6 MLDv1 snooping statistics.

Syntax

clear ipv6 mld statistics vlan *vlan-id*

Parameters

vlan*vlan-id*

Specifies the VLAN ID.

Modes

Privileged EXEC mode

Examples

To clear IPv6 MLDv1 snooping statistics for a specific VLAN:

```
device# clear ipv6 mld statistics vlan 100
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. On SLX 9140, the range is from 1 through 4096. On SLX 9240, the range is from 1 through 3566.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ipv6 nd suppression-statistics

Clears neighbor discovery (ND)-suppression statistical information. You can also clear statistics for a specified 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. On SLX 9140, the range is from 1 through 4096. On SLX 9240, the range is from 1 through 3566.

vlan *vlan-id*
Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example clears all ND-suppression statistics.

```
device#  clear ipv6 nd suppression-statistics
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ipv6 neighbor

Removes entries from the IPv6 neighbor table.

Syntax

clear ipv6 neighbor [*ipv6-address*] [**ethernet** *slot/port* | **ve** *ve-number*] [**force-delete** | **no-refresh** | **vrf** *vrf-name*]

Parameters

ipv6-address
Removes cache entries for the specified IPv6 address.

ethernet *slot/port*
Removes neighbor entries for the Ethernet interface. A valid slot number is 0.

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 0/1.

```
device# clear ipv6 neighbor ethernet 0/1 force-delete
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ipv6 ospf

Clears OSPFv3 data processes, counts, force-spf, neighbors, redistribution, routes, and traffic.

Syntax

clear ipv6 ospf all [**vrf** *vrf-name*]

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* | **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* | **ve** *vlan_id* } [*A.B.C.D*]

clear ipv6 ospf routes { *ipv6-addr* | **all** } [**vrf** *vrf-name*]

Parameters

all
Clears all OSPFv3 data.

counts
Clears OSPFv3 counters.

neighbor
Clears all OSPF 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. The slot number must be 0 if the switch does not contain slots.

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.

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.

ipv6-addr
Specifies an IPv6 address.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ipv6 route

Clears IPv6 routes.

Syntax

clear ipv6 route [*ipv6-address* **vrf** *vrf-name*] [**all vrf** *vrf-name*] [**slot** *slot-number*]

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 *slot-number*
Removes IPv6 routes for the specified slot. The valid slot number is 0.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

interface
Specifies an interface.

ethernet *slot port*
Specifies a valid, physical Ethernet interface with a slot and port number. The slot number must be 0 if the switch does not contain slots.

ve *vlan_id*
Specifies the VE VLAN number. The range is from 1 through 4096.

session *VRID*
Specifies the virtual group ID on which to clear statistics. The range is from 1 through 128.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Valid values range from 1 through 6144.

counters

Clears traffic counters.

Modes

Privileged EXEC mode

Examples

To clear the LACP counters for a specific port-channel:

```
device# clear lacp 10 counters
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

interface ethernet

Use this parameter to specify an Ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

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 ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear lldp statistics

Clears Link Layer Discovery Protocol (LLDP) statistics for all interfaces or a specified Ethernet interface.

Syntax

clear lldp statistics [**interface ethernet** *slot/port*]

Parameters

interface ethernet

Use this parameter to specify an Ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

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 ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

clear mac-address-table dynamic address *mac-address*

clear mac-address-table dynamic bridge-domain [*id*]

clear mac-address-table dynamic interface { **ethernet** *slot/port* } | { **port-channel** *number* }

clear mac-address-table dynamic logical-interface ethernet *0/port. lif-id*

clear mac-address-table dynamic vlan *vlan-id*

Parameters

cluster *cluster-id*
Specifies clearing MAC addresses from an MCT cluster ID. The ID range is 1-65535.

client *client-id*
Specifies clearing the client instance. The ID range is 1-512.

dynamic
Specifies the clearing of the specified MAC address, interface,

address *MAC-address*
Specifies clearing the dynamic MAC address. The valid format is *H.H.H* (available in Privileged EXEC mode only).

bridge-domain
Specifies clearing MAC addresses learned under bridge domains or a specified bridge-domain identifier.

interface
Specifies the clearing of the specified interface.

ethernet *0/port*
Specifies clearing the Ethernet interface with a valid port number.

port-channel *number*
Specifies clearing the port channel interface number. The range is from 1-1024 based on the platform.

logical-interface ethernet *0/port. lif-id*
Specifies clearing the logical ethernet interface on a specified port number.

vlan *vlan id*
Specifies clearing the VLAN interface. The VLAN ID range is from 1-4090.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear policy-map-counters

Provides a mechanism for clearing the policy map counters.

Syntax

clear policy-map-counters system [*map-name*]

clear policy-map-counters interface ethernet 0/*port* [**in** | **out**]

clear policy-map-counters interface port-channel *channel-number* [**in** | **out**]

Parameters

system *map-name*
Specifies the map name for the system statistics.

interface
Specifies an interface.

ethernet
Represents a valid, physical Ethernet type for all available Ethernet speeds.

0/*port*
Specifies a port number (this switch does not support a slot number, so "0" is used.).

port-channel *channel-number*
Represents a port channel.

in
Specifies clearing the ingress counters.

out
Specifies clearing the egress counters.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command with a specific interface and direction to clear the policy map counters for that interface.

Use this command without identifying an interface and direction of traffic to clear all of the policy map counters.

Examples

To clear the policy map counters for a specific interface use the following command:

```
device# clear policy-map-counters interface ethernet 0/2
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear ptp counter interface

Clears Precision Time Protocol (PTP) counters on all PTP-enabled interfaces or on a specified interface.

Syntax

clear ptp counter interface [*interface*]

Parameters

interface

Name of a PTP-enabled interface.

Modes

Privileged EXEC mode

Usage Guidelines

If no interface is specified, counters are cleared on all PTP-enabled interfaces on the switch.

Examples

To clear counters on all PTP-enabled interfaces on the switch:

```
device# clear ptp counter interface
```

To clear counters on a specified PTP-enabled interface:

```
device# clear ptp counter interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The number of available channels ranges from 1 through 6144.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The number of available channels ranges from 1 through 6144.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 2.

```
device# clear statistics bridge-domain 1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

clear tunnel statistics

Clears statistics from the tunnel interfaces.

Syntax

clear tunnel statistics *tunnel-id*

clear tunnel statistics mode [*gre* | *vxlan*]

clear tunnel statistics overlay-gateway *overlay-gateway-name*

Parameters

tunnel-id
Specifies the tunnel ID.

mode
Specifies the tunnel ID.

gre
Specifies GRE tunnels.

vxlan
Specifies VXLAN tunnels.

overlay-gateway *overlay-gateway-name*
Filters by Overlay gateway name.

Modes

Privileged EXEC mode

Examples

This example removes statistics from a tunnel interface.

```
device# clear tunnel statistics 10
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The slot number must be 0 if the switch does not contain slots.

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 0/6.

```
device# clear vrrp statistics interface ethernet 0/6
```

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 Extreme CLI syntax and Python syntax include the following differences:

- Although in general, Extreme 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 an Extreme 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 3.3.2 (default, Apr 11 2014, 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.

```
#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'^(\S+)\s+(\S+)\s+(\S+)\s+ACTIVE.*$', line, re.M)
    if found:
        slot_firmware[found.group(1)] = found.group(3)

print("SLOT_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 3.3.2 (default, Apr 11 2014, 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 to a Python variable and runs that command.

```
device# python
Python 3.3.2 (default, Apr 11 2014, 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')
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 65535.

Modes

Cluster client configuration mode

Usage Guidelines

The **no** form of the command removes the 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 MCT1-client 200
device(config-cluster-client-200)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

client-interface

Configures a client interface to the cluster client instance.

Syntax

client-interface { **ethernet 0/***port* | **port-channel** *number* }

no client-interface

Parameters

ethernet 0/*port*

Configures the specified Ethernet port as the client interface.

port-channel *number*

Configures the specified port channel as the client interface. 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.

You cannot configure a Layer 3 interface as an MCT client interface.

Examples

The following example shows how to configure a client interface.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# client-interface port-channel 3
```

History

Release version	Command history
17s.1.00	This command was introduced.

client-interfaces-shutdown

Disables the local client interfaces administratively in the cluster to moves all the traffic on the device to remote MCT peer device, resulting in fail-over of traffic to the peer device.

Syntax

client-interfaces-shutdown

no client-interfaces-shutdown

Modes

Cluster configuration mode

Usage Guidelines

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# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# client-interfaces-shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

client-isolation-strict

Sets the client-isolation mode to strict when the EVPN control session goes down between the MCT devices for Broadcast, Unknown unicast and Multicast (BUM) handling over client interfaces.

Syntax

client-isolation-strict

no client-isolation-strict

Command Default

By default, client-isolation mode is loose.

Modes

Cluster configuration mode

Usage Guidelines

In strict mode, when the EVPN control session goes down, the interfaces on both the cluster devices are ports are not down. None of the ports are made DF. There is no impact to unicast traffic. However, only BUM forwarding is not done. In strict mode, the client is completely isolated from the network if the control session is not operational.

MCT cluster devices can operate in two modes. Both peer devices must be configured with the same mode configuration.

> NOTE
> The CLI allows modification of the client isolation mode on MCT cluster devices even when the cluster is deployed. You must have the same isolation mode configuration on both cluster devices.

The **no** form of the command resets the default client isolation mode of loose.

Examples

The following example shows how to configure strict client-isolation mode.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# client-isolation-strict
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 4pm in the afternoon on July 28, 2016, for the local device:

```
device# clock set ?
Possible completions:
  <dateTime (CCYY-MM-DDTHH:MM:SS)>
device# clock set 2017-03-22T22:10:30
device# Wed Mar 22 22:10:30 GMT 2017
```

History

Release version	Command history
17s.1.00	This command was introduced.

clock timezone

Sets the device system clock time zone options using a valid timezone region and city.

Syntax

clock timezone { *timezone-region* **/** *city* }

no clock timezone

Parameters

timezone-region/city

Specifies a timezone region and city.

Modes

Global configuration mode

Examples

The following example sets the system date and time to New York (Eastern) time.

```
device# configure terminal
device(config)# clock timezone ?
 timezone   timezone region/city (regions are Africa, America, Antarctica,
             Arctic, Asia, Atlantic, Australia, Europe, Indian, Pacific)
device(config)# clock timezone America/New_York
%%INFO: Reload is recommended to update all system entities with the configured time zone
```

History

Release version	Command history
17s.1.00	This command was introduced.

cluster

Configures a Multi-Chassis Trunking (MCT) cluster and accesses the cluster configuration mode.

Syntax

cluster *cluster-name cluster-id*

no cluster *cluster-name cluster-id*

Parameters

cluster-name

Specifies the cluster name as an ASCII string. The cluster name can be up to 64 characters in length.

cluster-id

Specifies the cluster ID. The ID value range can be from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

NOTE

The *cluster-id* variable must be the same on both cluster devices.

The **no** form of the command removes the MCT cluster configuration.

Examples

The following example configures an MCT cluster.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

cluster management node-id

Configures a node ID for a node in an IP management cluster.

Syntax

cluster management node-id *node_ID*]

no cluster management node-id

Command Default

The default node ID is 1.

Parameters

node_ID

The node ID. Range is 1 through 255. Default is 1.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to revert to the default node ID.

Two nodes in a management cluster cannot have the same node ID.

The node ID persists after the execution of the **copy default-config startup-config** command and database corruption.

Examples

The following example changes the node ID to a nondefault value.

```
device# cluster management node-id 20
```

The following example restores the default value.

```
device# no cluster management node-id
```

History

Release version	Command history
17s.1.01	This command was introduced.

cluster management virtual

Assigns a single virtual IPv4 or IPv6 address to all switches in an IP-based management cluster.

Syntax

cluster management virtual { **ip address** *ipv4_address/prefix_len* **inband interface ve***VE_number* | **ipv6 address** *ipv6_address/prefix_len* }

no cluster management virtual ip address

no cluster management virtual ipv6 address

Parameters

ip address *ipv4_address/prefix_len*
Specifies the IPv4 address and prefix length means of a CIDR prefix (mask).

inband interface ve *VE_number*
Specifies a virtual Ethernet (VE) interface.

ipv6 address *ipv6_address/prefix_len*
Specifies the IPv6 address and prefix length means of a CIDR prefix (mask).

Modes

Global configuration mode

Usage Guidelines

When you configure the virtual IPv4 or IPv6 address for the first time, the address is assigned to the principal switch. You can then access the principal switch through the management port IP address or the virtual IP address. The virtual IP configuration is global in nature. All the nodes in the fabric will be configured with the same virtual IP address, but the address is always bound to the current principal switch.

This command can be used only after the fabric has formed successfully.

The command can be executed from any node. You can remove a virtual IP address when you are logged on to the switch through the virtual IP address. Use the management port IP address or the serial console to configure the virtual IP address.

The **inband interface ve**parameter can only be used when assigning an IPv4 address. This parameter is not applicable for IPv6 addresses.

It is the responsibility of the network administrator to ensure that the virtual IP address assigned is not a duplicate of an address assigned to any other management port in the fabric.

The virtual IP address should be configured on the same subnet as the management interface IP address.

Enter **no cluster management virtual ip address** or **no cluster management virtual ipv6 address** to remove a currently configured virtual IPv4 or IPv6 address, respectively.

Examples

The following example assigns a virtual IPv4 address and mask to the principal switch and specify a VE interface.

```
device# configure terminal
device(config)# cluster management virtual ip address 30.30.30.14/24 inband interface ve 4
```

The following example removes the currently configured virtual IPv4 address.

```
device(config)# no cluster management virtual ip address
```

The following example assigns a virtual IPv6 address and mask to the principal switch.

```
device(config)# vcs virtual ipv6 address 2001:db8::/64
```

History

Release version	Command history
17s.1.01	This command was introduced.

cluster-control-vlan

Configures the cluster control VLAN.

Syntax

cluster-control-vlan *VLAN_ID*

no cluster-control-vlan

Command Default

By default, the cluster control VLAN is 4090.

Parameters

VLAN_ID

Specifies the VLAN ID. Enter an integer from 1 through 4090.

Modes

Cluster configuration mode

Usage Guidelines

Use the **no** form of this command to reset the VLAN to the default value of 4090.

The cluster control VLAN is required for MAC learning, resolving ARP for the BGP peer, and to derive the outer MAC address for the NSH tunnel.

If MCT is configured, other switch ports must not be part of the cluster control VLAN.

You cannot configure the cluster control VLAN when the cluster is deployed.

Examples

The following example configures the cluster control VLAN of 35.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# cluster-control-vlan 35
```

History

Release version	Command history
17s.1.00	This command was introduced.

cluster-id

Configures a cluster ID for the route reflector.

Syntax

cluster-id { *num* | *ip-addr* }

no cluster-id { *num* | *ip-addr* }

Command Default

The default cluster ID is the device ID.

Parameters

num

Integer value for cluster ID. Range is from 1 through 65535.

ip-addr

IPv4 address in dotted-decimal notation.

Modes

BGP configuration mode

Usage Guidelines

When configuring multiple route reflectors in a cluster, use the same cluster ID to avoid loops within the cluster.

The **no** form of the command restores the default so that the cluster ID is the device ID.

Examples

The following example configures a cluster ID for the route reflector.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# cluster-id 1234
```

History

Release version	Command history
17s.1.00	This command was introduced.

cluster-system-id

Configures the last byte of the bridge ID to ensure that two or more MCT clusters do not have the same bridge IDs in a Layer 2 topology.

Syntax

cluster-system-id *last-byte*

Parameters

last-byte

Specifies the last byte of the bridge ID. Enter an integer from 1 to 255.

Modes

Spanning tree configuration mode

Usage Guidelines

The bridge ID (Switch MAC) used by all nodes participating in the STP domain should have unique MAC address.

This command is applicable only if the cluster is configured.

You must configure the same value in both cluster nodes.

Ensure that the global STP configuration is consistent on both cluster nodes. Configuration mismatch handling is not supported.

Examples

The following example configures the last byte of the bridge ID to 2.

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(config-rstp)# cluster-system-id 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command restores the default so that the device does not compare MEDs for internal routes that originate within the local AS or confederation.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Usage Guidelines

The **no** form of the command disables the comparison of device IDs.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Use this command to configure a single AS number to identify a group of smaller autonomous systems as a single confederation.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

configure terminal

Enters global configuration mode.

Syntax

configure terminal

Modes

Privileged EXEC mode

History

Release version	Command history
17s.1.00	This command was introduced.

connector

Accesses connector configuration mode for the Ethernet port.

Syntax

connector *slot/port*

Parameters

slot/port

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

Modes

Hardware configuration mode

Usage Guidelines

In connector configuration mode, you can break out the port into four 10G ports.

Examples

The following example shows the accessing of the connector configuration mode.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# connector 0/2
device(config-connector-0/2)# breakout mode 4x10g
```

History

Release version	Command history
17s.1.00	This command was introduced.

continue

Configures a route-map instance number that goes in a continue statement in a route-map instance.

Syntax

continue *number*

no continue *number*

Parameters

number

Route-map instance number. Range is from 1 through 4294967295.

Modes

Global configuration mode

Usage Guidelines

Use the **no continue** *number* command to disable the instance number.

Examples

Typical command example:

```
device# configure terminal
device(config)# continue 8675309
```

History

Release version	Command history
17s.1.00	This command was introduced.

copy

Copies configuration data.

Syntax

copy *source_file destination_file*

Parameters

source_file

The source file to be copied. Specify one of the following parameters:

default-config
The default configuration.

default-profile
The default profile 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.

running-config
The running configuration.

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.

startup-config
The startup configuration.

support
The support data.

support-interactive
The interactive mode.

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.

user-defined-profile*path*
The user defined profile configuration.

destination_file

The destination file. Specify one of the following parameters:

default-config
The default 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.

startup-config
The startup configuration.

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.

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".

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

crypto ca authenticate

Downloads the certification authority (CA) certificate for a trustpoint from a remote certificate server for authentication purposes.

Syntax

crypto ca authenticate *trustpointCA_name* { **directory** *remote_dir_name* | **file** *cert_file* | **host** *host_address* | **password** *host_user_password* | **protocol** { **FTP** | **SCP** } | **user** *host_login* }

no crypto ca authenticate { *trustpointCA_name* }

Parameters

trustpointCA_name
Specifies a trustpoint name. The trustpoint name can range from 1 through 64 characters in length.

directory *remote_dir_name*
Specifies the directory where the certification file resides.

file *cert_file*
Specifies the name of the certification file in Privacy Enhanced Mail (PEM) format.

host *host_address*
Specifies the remote certificate server in hostname or IP address format.

password *host_user_password*
Specifies the password for the user name on the host server.

NOTE
For security purposes, it is recommended that the password is not listed in the command line; the user will be prompted to enter the password.

protocol
Specifies the protocol for accessing the certification file.

FTP
Specifies using File Transfer Protocol.

SCP
Specifies using Secure Copy Protocol.

user *host_login*
Specifies the user name for login to the host server.

Modes

Privileged EXEC mode

Usage Guidelines

The CA certificate downloaded from the trusted CA is used to sign the certificate signing request (CSR) and generate the identity certificate.

Before issuing the **crypto ca authenticate** command for a trustpoint, the trustpoint must be created by using the **crypto ca trustpoint** command.

The *trustpoint_CAname* 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 delete the certificate.

Examples

The following example shows how to authenticate the certificate authority certificate for a trustpoint named t1.

```
device# crypto ca authenticate t1 protocol SCP host 10.70.12.102 user fvt directory /users/home/crypto
file cacert.pem

Password: **********
```

History

Release version	Command history
17s.1.00	This command was introduced.

crypto ca enroll

Enrolls a trustpoint by generating the certificate signing request (CSR) and exporting it to the remote certificate authority (CA) server.

Syntax

crypto ca enroll *trustpointCA_name* { **common** *common_name* | **country** *country* | **directory** *remote_dir_name* | **host** *host_address* | **locality** *locality* | **organization** *organization* | **orgunit** *orgunit* | **password** *host_user_password* | **protocol** { **FTP** | **SCP** } | **state** *state* | **user** *host_login* }

Parameters

trustpointCA_name
Specifies a trustpoint name. The trustpoint name can range from 1 through 64 characters in length.

common *common_name*
Specifies the common 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. The common name can range from 1 through 253 characters in length.

country *country*
Specifes the two-letter country code for generating the CSR.

directory *remote_dir_name*
Specifies the remote directory to which the CSR is exported.

host *host_address*
Specifies the remote certificate server in hostname or IP address format.

locality *locality*
Specifies the locality name for generating the CSR.

organization *organization*
Specifies the organization name for generating the CSR.

orgunit *orgunit*
Specifies the organization subunit name for generating the CSR.

password *host_user_password*
Specifies the password for the user name on the host server.

NOTE
For security purposes, it is recommended that the password is not listed in the command line; the user will be prompted to enter the password.

protocol
Specifies the protocol to use for exporting the certification file.

FTP
Specifies using File Transfer Protocol.

SCP
Specifies using Secure Copy Protocol.

state *state*
Specifies the state name for generating the CSR.

user *host_login*
Specifies the user name for login to the host server.

Modes

Privileged EXEC mode

Usage Guidelines

Before issuing the **crypto ca enroll** command for a trustpoint, the trustpoint must be created by using the **crypto ca trustpoint** command.

Examples

The following example shows how to enroll a trustpoint named t1 on a certificate authority server that is identified by the IP address 10.70.12.102.

```
device# crypto ca enroll t1 country US state CA locality SJ organization BRC orgunit SFI common
myhost.example.com protocol SCP host 10.70.12.102 user fvt directory /proj/crypto
Password: **********
```

History

Release version	Command history
17s.1.00	This command was introduced.

crypto ca import

Imports an identity certificate for HTTPS security configuration.

Syntax

crypto ca import *trustpointCA_name* **certificate** { **directory** *remote_dir_name* | **file** *cert_file* | **host** *host_address* | **password** *host_user_password* | **protocol** { **FTP** | **SCP** } | **user** *host_login* }

no crypto ca import { *trustpointCA_name* }

Parameters

trustpointCA_name
Specifies a trustpoint name. The trustpoint name can range from 1 through 64 characters in length.

certificate
Causes the import of an identity certificate.

directory *remote_dir_name*
Specifies the directory where the certification file resides.

file *cert_file*
Specifies the name of the certification file.

host *host_address*
Specifies the host name or IP address of the remote certificate server.

password *host_user_password*
Specifies the password for the user name on the host server.

NOTE
For security purposes, it is recommended that the password is not listed in the command line; the user will be prompted to enter the password.

protocol
Specifies the protocol for importing the certification file.

FTP
Specifies using File Transfer Protocol.

SCP
Specifies using Secure Copy Protocol.

user *host_login*
Specifies the user name for login to the host server.

Modes

Privileged EXEC mode

Usage Guidelines

Before issuing the **crypto ca import** command for a trustpoint, the trustpoint must be created by using the **crypto ca trustpoint** command.

The **no** form of the command deletes the identity certificate.

Examples

The following example shows how to import an identity certificate file for a trustpoint named t1 from a remote certificate server identified by the IP address 10.70.12.102.

```
device# crypto ca import t1 certificate protocol SCP host 10.70.12.102 user fvt directory /users/crypto
file cacert.pem

Password: **********
```

History

Release version	Command history
17s.1.00	This command was introduced.

crypto ca trustpoint

Creates a trustpoint for HTTPS security configuration and enters configuration mode for the trustpoint.

Syntax

crypto ca trustpoint *trustpointCA_name*

no crypto ca trustpoint *trustpointCA_name*

Parameters

trustpointCA_name

Specifies a trustpoint name. The trustpoint name can range from 1 through 64 characters in length.

Modes

Global configuration mode

Usage Guidelines

The **no** version of the command removes the trustpoint configuration.

Examples

The following example shows how to create a trustpoint named t1 and enter configuration mode for the trustpoint.

```
device# configure terminal
device(config)# crypto ca trustpoint t1
device(config-ca-t1)#
```

The following example shows how to remove the t1 trustpoint configuration from the device.

```
device# configure terminal
device(config)# no crypto ca trustpoint t1
```

History

Release version	Command history
17s.1.00	This command was introduced.

crypto key

Generates a cryptographic key pair for use in security protocol exchanges for applications.

Syntax

crypto key label *key_label* { **dsa** | **ecdsa** | **rsa** } [**modulus** *key_size*]

no crypto key label *key_label*

Parameters

label *key_label*
: Specifies the cryptographic keypair label in alphanumeric characters.

dsa
: Generates a Digital Signature Algorithm (DSA) keypair.

ecdsa
: Generates an Elliptic Curve Digital Signature Algorithm (ECDSA) keypair.

rsa
: Generates a Rivest, Shamir and Adelman (RSA) keypair.

modulus *key_size*
: Specifies the key size. The corresponding key sizes supported for each keypair type are:

- RSA: 1024 or 2048 bits
- DSA: 1024 bits
- ECDSA: 256, 384, or 521 bits

Modes

Global configuration mode

Usage Guidelines

You must sign and encrypt or decrypt the key pair before you obtain a certificate for your device.

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

Examples

The following example shows how to generate an RSA keypair labeled k1 with a key size of 2048 bits.

```
device# configure terminal
device(config)# crypto key label k1 rsa modulus 2048
```

The following example shows how to remove the k1 keypair configuration.

```
device# configure terminal
device(config)# no crypto key label k1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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-name* }

no dampening

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
Name of the configured route map.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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.

The **no** form of the command disables dampening.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

database-overflow-interval (OSPFv2)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

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. The default is 0 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.

If the device enters OverflowState, you must reboot before the device leaves this state.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

database-overflow-interval (OSPFv3)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

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). The default is 10 seconds.

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.

If the router enters OverflowState, you must reboot before the router leaves this state.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Please work closely with Extreme Networks technical support in 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel interface. The range is from 1 through 6144.

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. Please work closely with Extreme Networks technical support in 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 0/5.

```
device# debug arp packet buffer interface ethernet 0/5 tx
```

The following command disables ARP packet capture on all interface.

```
device# no debug arp packet buffer all
```

History

Release version	Command history
17s.1.00	This command was introduced.

debug dhcp packet buffer

Configures a buffer to capture DHCP packets.

Syntax

debug dhcp packet buffer all

no debug dhcp packet buffer all

debug dhcp packet buffer { **circular** | **linear** } **packet-count** *num-packets* [**vrf** *vrf-name*]

debug dhcp packet buffer clear [**vrf** *vrf-name*]

debug dhcp packet buffer interface { **ethernet** *slot* **/** *port* | **port-channel** *number* } [**rx** | **tx**]

no debug dhcp packet buffer interface { **ethernet** *slot* **/** *port* | **port-channel** *number* } [**rx** | **tx**]

Command Default

The buffer wraps around to overwrite earlier captures (circular).

Parameters

all
Captures DHCP packets on all interfaces.

circular
Buffer wraps around to overwrite earlier captures.

linear
Buffer does not wrap around to overwrite earlier captures.

packet-count *num-packets*
Specifies a value from 64 through 2056.

vrf *vrf-name*
Specifies a VRF.

clear
Clears the packet buffer.

interface
Represents an Ethernet or port-channel interface.

ethernet
Specifies a physical 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 interface. The range is from 1 through 6144.

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. Please work closely with Extreme Networks technical support in 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 a **no** form of this command to disable DHCP debugging. You can specify an interface or all interfaces.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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. Please work closely with Extreme Networks technical support in 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
```

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Please work closely with Extreme Networks technical support in 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Please work closely with Extreme Networks technical support in 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* }

no debug ip igmp

Parameters

all
Enables all debugs.

errors
Enables only error type debugs, such as memory allocation failures etc.

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 query/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 me monitored.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in 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.

Use the **no** form of this command to disable debugging.

History

Release version	Command history
17s.1.00	This command was introduced.

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-prefix
Displays information filtered by IPv6 prefix.

ipv6-address /mask
Specifies an IPv6 address and network mask.

name
Specifies a prefix list name.

all-vrfs
Specifies all VRFs.

vrf
Specifies a VRF instance or all VRFs.

vrf-name
Specifies a VRF instance

ipv6-prefix-list
Displays information filtered by IPv6 prefix list.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

The **no** form of the command disables debugging.

Examples

The following example enables debugging for IPv6 prefix list "myv6list" for VRF instance "red".

```
device# debug ipv6 bgp ipv6-prefix-list myv6list vrf red
```

The following example enables debugging for a specified IPv6 address for all VRFs.

```
device# debug ipv6 bgp ipv6-prefix 2001::/16 all-vrfs
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Please work closely with Extreme Networks technical support in 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

debug lacp

Enables or disables debugging for the Link Aggregation Control Protocol (LACP).

Syntax

debug lacp { **all** | **cli** | **event** | **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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Examples

Typical use of this command.

```
device# debug lldp dump all
LLDP Interface Debug Information for 0/2
Admin Status:  RX_TX
Associated Profile:
Link-level iSCSI Priority: 0x10 (Configured: No)
Link Properties:
    CEE Incapable
    FCF-Forward Disabled
Sending TLVs:
    CHASSIS_ID: 0x50eb1a173ff1 (MAC)
    PORT_ID: 0/2 (IF Name)
    TTL: Hold (4) x Interval (30)
    SYSTEM_NAME
    IEEE_DCBX
    DCBX_CTRL
<truncated>
```

History

Release version	Command history
17s.1.00	This command was introduced.

debug lldp packet

Enables or disables debugging for the Link Layer Discovery Protocol (LLDP).

Syntax

debug lldp packet { **all** { **both** | **rx** | **tx** } | **ethernet** *slot/port* { **both** | **rx** | **tx** } } | [**detail**]

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. The only valid value is 0.

port

Specifies a valid port number.

both

Turns on 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.

detail

Turns on debugging with detailed information.

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 all interfaces:

```
device# debug lldp packet all both detail
device# show debug lldp
Interface Eth 0/1  : Receive Transmit Detail
Interface Eth 0/2  : Receive Transmit Detail
Interface Eth 0/3  : Receive Transmit Detail
Interface Eth 0/4  : Receive Transmit Detail
Interface Eth 0/5  : Receive Transmit Detail
Interface Eth 0/6  : Receive Transmit Detail
Interface Eth 0/7  : Receive Transmit Detail
Interface Eth 0/8  : Receive Transmit Detail
Interface Eth 0/9  : Receive Transmit Detail
Interface Eth 0/10  : Receive Transmit Detail
Interface Eth 0/11  : Receive Transmit Detail
Interface Eth 0/12  : Receive Transmit Detail
Interface Eth 0/13  : Receive Transmit Detail
Interface Eth 0/14  : Receive Transmit Detail
Interface Eth 0/15  : Receive Transmit Detail
Interface Eth 0/16  : Receive Transmit Detail
Interface Eth 0/17  : Receive Transmit Detail
Interface Eth 0/18  : Receive Transmit Detail
Interface Eth 0/19  : Receive Transmit Detail
Interface Eth 0/20  : Receive Transmit Detail
Interface Eth 0/21  : Receive Transmit Detail
Interface Eth 0/22  : Receive Transmit Detail
Interface Eth 0/23  : Receive Transmit Detail
Interface Eth 0/24  : Receive Transmit Detail
Interface Eth 0/25  : Receive Transmit Detail
Interface Eth 0/26  : Receive Transmit Detail
Interface Eth 0/27  : Receive Transmit Detail
Interface Eth 0/28  : Receive Transmit Detail
Interface Eth 0/29  : Receive Transmit Detail
Interface Eth 0/30  : Receive Transmit Detail
Interface Eth 0/31  : Receive Transmit Detail
Interface Eth 0/32  : Receive Transmit Detail
```

To enable debugging of LLDP for both received and transmitted packets on 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The number of available channels ranges from 1 through 6144.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 disables the advertisement of a default route.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

default-metric (BGP)

Changes the default metric used for redistribution.

Syntax

default-metric *value*

no default-metric

Parameters

value

Metric value. Range is from 0 through 4294967295. The default is 1.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 will use 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)# rrouter ospf
device(config-router-ospf-vrf-default-vrf)# default-metric 20
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 configures Ethernet interface 0/2 to delay transmission of port down events to Layer 2 protocols.

```
device# configure terminal
device(config)# interface Ethernet 0/2
device(conf-if-eth-0/2)# delay-link-event 2 down
```

History

Release version	Command history
17s.1.00	This command was introduced.

delay-request-min-interval

Configures on a slave port the minimum interval allowed between Precision Time Protocol (PTP) Delay-Request messages sent on the port.

Syntax

delay-request-min-interval *seconds*

no delay-request-min-interval

Parameters

seconds

Interval between PTP Delay-Request messages, in log seconds. 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 $1/(2^{\log \text{seconds}})$.

Configuring this interval on an edge port overrides the switch (global) default.

ATTENTION
Do not configure a rate slower than the default on links between Extreme SLX-OS devices.

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

Examples

To configure a PTP Delay-Request minimum 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)# delay-request-min-interval 2
```

To revert to the default minimum 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 delay-request-min-interval
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

deny inner-gtp-https

Enables the dropping—from ingress traffic—of GPRS Tunneling Protocol (GTP) frames that encapsulate HTTPS packets.

Syntax

deny inner-gtp-https

no deny inner-gtp-https

Command Default

Such filtering is not enabled.

Modes

Interface configuration mode

Usage Guidelines

This feature must be implemented per physical interface.

This feature applies to GTP v.1 frames.

If this feature filtering is enabled, common practice is to forward the filtered traffic by using a Network Packet Broker (NPB) route-map.

The **no** form of this command disables this feature.

Examples

The following example enables dropping GTP frames that encapsulate HTTPS packets.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# deny inner-gtp-https
```

The following example restores the default setting of not dropping HTTPS packets transported within GTP frames.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# no deny inner-gtp-https
```

History

Release version	Command history
17s.1.02	This command was introduced.

deploy

Deploys the MCT cluster or cluster client to bring the MCT device to operational mode.

Syntax

deploy

no deploy

Modes

Cluster and cluster client configuration mode

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.

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 the client cluster.

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# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# deploy
```

The following example shows the deployment of a cluster client.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# deploy
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.
```

History

Release version	Command history
17s.1.00	This command was introduced.

description (interfaces)

Specifies a string describing an 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 0/2:

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# description converged_101
```

History

Release version	Command history
17s.1.00	This command was introduced.

description (LLDP)

Specifies a string that contains the LLDP description.

Syntax

description *string*

Parameters

string

Characters describing LLDP. The string must be between 1 and 50 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Profile configuration mode

Usage Guidelines

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# configure terminal
device(config)# protocol lldp
device(conf-lldp)# description Bro-LLDP
```

To set the strings describing LLDP for a specific LLDP profile, test2, enter the following:

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# profile test1
device(config-profile-test1)# description test2
device(config-profile-test1)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

description (TVF domain)

Describes a Transparent VLAN flooding (TVF) domain.

Syntax

description *description-text*

description

Command Default

TVF domains have no description.

Parameters

description-text
Describes a TVF domain.

Modes

TVF-domain configuration mode

Usage Guidelines

To remove a description, enter the command with no *description-text*.

To modify a description, enter the full **description** *description-text* command. You do not need to first remove the previous description.

Examples

The following example creates a TVF domain and then adds a description.

```
device# configure terminal
device(config)# tvf-domain 10
device(config-tvf-domain-10)# description Sample TVF domain
```

The following example displays current TVF domains and their descriptions, accesses a TVF domain, changes its description, and then displays the modifed description.

```
device# show running-config tvf-domain
tvf-domain 1
!
tvf-domain 10
description Sample TVF domain
!

device# configure terminal
device(config)# tvf-domain 10
device(config-tvf-domain-10)# description Enterprise TVF domain

device(config-tvf-domain-10)# do show running-config tvf-domain
tvf-domain 1
!
tvf-domain 10
description Enterprise TVF domain
```

History

Release version	Command history
18s.1.00	This command was introduced.

description (VRRP)

Describes a Virtual Router Redundancy Protocol (VRRP) or a VRRP 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

This command can be used in both VRRP and VRRP-E. 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 leaf node in a set of multi-homing nodes 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 client is configured. When a client 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# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# designated-forwarder-hold-time 20
```

History

Release version	Command history
17s.1.01	This command was introduced.

destination

Designates the destination interface for the snooping data for flow-based SPAN.

Syntax

destination *dest_ifname*

no destination *dest_ifname*

Parameters

dest_ifname

The name of the destination interface.

Modes

Monitor session mode

Usage Guidelines

Use the **no destination** *dest_ifname* command to delete the destination interface.

Examples

This example configures the IP address Ethernet 0/1 as the destination address.

```
device# configure terminal
device(config)# monitor session 22
switch(config-session-22)# destination ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

df-load-balance

Enables designated forwarder (DF) load balancing.

Syntax

df-load-balance

no df-load-balance

Command Default

By default, DF load balancing is disabled.

Modes

Cluster configuration mode

Usage Guidelines

Use the **no** form of the command to disable DF load balancing.

One leaf node is the DF for the VLAN on the Ethernet segment (ES).

When DF load balancing is disabled, DF election is triggered only when the current DF leaf node goes down or its client interface is down. When a non-DF leaf node goes down or a new node joins the ES, DF election is not triggered.

When DF load balancing is enabled, the DF election is triggered in the following scenarios:

- A client is deployed locally or remotely.
- The BGP cluster control protocol (CCP) session comes up.
- Remote CCEP goes up or down.

Examples

The following example enables the load balancing of the designated forwarder.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# df-load-balance
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

NOTE

If you need to interrupt the ZTP operation when in progress using the **dhcp ztp cancel** command, you may notice a one minute delay in canceling.

Once canceled, the ZTP session stops retry, irrespective of whether the process succeeds or fails. If firmware download completes successfully, the device returns to the normal mode. The following limitations apply:

- If firmware download has not started, you will need to reboot the switch manually to bring the switch back to normal mode.
- If firmware download has already started, you must wait for firmware download to complete before running any other CLI, power cycling the switch, starting a new firmware download, or starting a new ZTP session.
- If 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 after device bootup.

```
device# dhcp ztp cancel
Warning: This command will terminate the existing ZTP session
Do you want to continue? [y/n] y
```

The following output displays if ZTP is not enabled

```
device# dhcp ztp cancel
ZTP is not enabled.
```

If you force the cancellation of ZTP while in progress, the following output displays.

```
device# dhcp ztp cancel
Warning: This command will terminate the existing ZTP session
After ZTP has been confirmed canceled, you need to run "reload system" before configuring the switch.
Do you want to continue? [y/n] y
```

History

Release version	Command history
17s.1.00	This command was introduced.

dhcp ztp log

Displays the Zero Touch Provisioning progress log.

Syntax

dhcp ztp log

Command Default

Modes

Privileged EXEC mode

Usage Guidelines

The progress log displays if Zero Touch Provisioning is enabled.

Examples

The following log displays if ZTP cancels successfully.

```
device# dhcp ztp log
ZTP, Mon Sep 11 14:32:56 2000, ========== ZTP start ==========
ZTP, Mon Sep 11 14:32:56 2000, disable raslog
ZTP, Mon Sep 11 14:32:56 2000, CLI is ready
ZTP, Mon Sep 11 14:33:23 2000, inband ports are enabled
ZTP, Mon Sep 11 14:33:23 2000, serial number = EXG3326M00P
ZTP, Mon Sep 11 14:33:23 2000, model name = SLX9240
ZTP, Mon Sep 11 14:33:23 2000, use both management inteface and inband interfaces
ZTP, Mon Sep 11 14:33:23 2000, checking inband interfaces link status
ZTP, Mon Sep 11 14:33:23 2000, find link up on intefaces: eth0
ZTP, Mon Sep 11 14:33:23 2000, start dhcp process on interfaces: eth0
ZTP, Mon Sep 11 14:33:27 2000, interface eth0 receives dhcp response
ZTP, Mon Sep 11 14:33:27 2000, ping ftp server 192.168.1.1
ZTP, Mon Sep 11 14:33:28 2000, ping succeed
ZTP, Mon Sep 11 14:33:28 2000, download ZTP config file from ftp://192.168.1.1/config/ztp.cfg
ZTP, Mon Sep 11 14:33:28 2000, receive ZTP configuration file [ztp.cfg]
ZTP, Mon Sep 11 14:33:28 2000, interface eth0 connectivity test pass
ZTP, Mon Sep 11 14:33:29 2000, download script file [dad1_new.py]
ZTP, Mon Sep 11 14:33:29 2000, download switch config file [cedar_ospf.cfg]
ZTP, Mon Sep 11 14:33:29 2000, ZTP configuration sanity check pass
ZTP, Mon Sep 11 14:33:29 2000, skip firmware upgrade, switch reboot in 5 seconds
ZTP, Mon Sep 11 14:33:29 2000, ZTP is canceled
ZTP, Mon Sep 11 14:33:29 2000, enable raslog
ZTP, Mon Sep 11 14:33:29 2000, ========== ZTP completed ==========
```

If the device has the same image as the ZTP configuration file, the following output displays:

```
device# dhcp ztp log
ZTP, Fri Mar 17 15:46:51 2017, ========== ZTP start ==========
ZTP, Fri Mar 17 15:46:51 2017, disable raslog
ZTP, Fri Mar 17 15:46:51 2017, CLI is ready
ZTP, Fri Mar 17 15:47:19 2017, inband ports are enabled
ZTP, Fri Mar 17 15:47:19 2017, serial number = EXH3327M014
ZTP, Fri Mar 17 15:47:19 2017, model name = SLX9140
ZTP, Fri Mar 17 15:47:19 2017, use both management inteface and inband interfaces
ZTP, Fri Mar 17 15:47:19 2017, checking inband interfaces link status
ZTP, Fri Mar 17 15:48:10 2017, find link up on intefaces: eth0 Eth0.9 Eth0.10 Eth0.11
ZTP, Fri Mar 17 15:48:10 2017, start dhcp process on interfaces: eth0 Eth0.9 Eth0.10 Eth0.11
ZTP, Fri Mar 17 15:48:15 2017, interface eth0 receives dhcp response
ZTP, Fri Mar 17 15:48:15 2017, ping ftp server 192.168.1.1
ZTP, Fri Mar 17 15:48:16 2017, ping succeed
ZTP, Fri Mar 17 15:48:16 2017, download ZTP config file from ftp://192.168.1.1/config/ztp.cfg
ZTP, Fri Mar 17 15:48:16 2017, receive ZTP configuration file [ztp.cfg]
ZTP, Fri Mar 17 15:48:16 2017, interface eth0 connectivity test pass
ZTP, Fri Mar 17 15:48:17 2017, download script file [FreedomZTP.py]
ZTP, Fri Mar 17 15:48:17 2017, download switch config file [freedom_ospf.cfg]
ZTP, Fri Mar 17 15:48:17 2017, ZTP configuration sanity check pass
ZTP, Fri Mar 17 15:48:17 2017, skip firmware upgrade, switch reboot in 5 seconds
ZTP, Fri Mar 17 15:51:46 2017, ========== ZTP continue ==========
ZTP, Fri Mar 17 15:51:46 2017, disable raslog
ZTP, Fri Mar 17 15:51:46 2017, CLI is ready
ZTP, Fri Mar 17 15:52:11 2017, replay config file...
ZTP, Fri Mar 17 15:52:21 2017, running configuration script [FreedomZTP.py]
ZTP, Fri Mar 17 15:58:28 2017, commit configuration
ZTP, Fri Mar 17 15:58:28 2017, ZTP succeed
ZTP, Fri Mar 17 15:58:28 2017, enable raslog
ZTP, Fri Mar 17 15:58:28 2017, ========== ZTP completed ==========
```

The following output displays if ZTP is successful:

```
device# dhcp ztp log
ZTP, Fri Mar 17 15:46:51 2017, ========== ZTP start ==========
ZTP, Fri Mar 17 15:46:51 2017, disable raslog
ZTP, Fri Mar 17 15:46:51 2017, CLI is ready
ZTP, Fri Mar 17 15:47:19 2017, inband ports are enabled
ZTP, Fri Mar 17 15:47:19 2017, serial number = EXH3327M014
ZTP, Fri Mar 17 15:47:19 2017, model name = SLX9140
ZTP, Fri Mar 17 15:47:19 2017, use both management inteface and inband interfaces
ZTP, Fri Mar 17 15:47:19 2017, checking inband interfaces link status
ZTP, Fri Mar 17 15:48:10 2017, find link up on intefaces: eth0 Eth0.9 Eth0.10 Eth0.11
ZTP, Fri Mar 17 15:48:10 2017, start dhcp process on interfaces: eth0 Eth0.9 Eth0.10 Eth0.11
ZTP, Fri Mar 17 15:48:15 2017, interface eth0 receives dhcp response
ZTP, Fri Mar 17 15:48:15 2017, ping ftp server 192.168.1.1
ZTP, Fri Mar 17 15:48:16 2017, ping succeed
ZTP, Fri Mar 17 15:48:16 2017, download ZTP config file from ftp://192.168.1.1/config/ztp.cfg
ZTP, Fri Mar 17 15:48:16 2017, receive ZTP configuration file [ztp.cfg]
ZTP, Fri Mar 17 15:48:16 2017, interface eth0 connectivity test pass
ZTP, Fri Mar 17 15:48:17 2017, download script file [FreedomZTP.py]
ZTP, Fri Mar 17 15:48:17 2017, download switch config file [freedom_ospf.cfg]
ZTP, Fri Mar 17 15:48:17 2017, ZTP configuration sanity check pass
ZTP, Fri Mar 17 15:48:17 2017, skip firmware upgrade, switch reboot in 5 seconds
ZTP, Fri Mar 17 15:51:46 2017, ========== ZTP continue ==========
ZTP, Fri Mar 17 15:51:46 2017, disable raslog
ZTP, Fri Mar 17 15:51:46 2017, CLI is ready
ZTP, Fri Mar 17 15:52:11 2017, replay config file...
ZTP, Fri Mar 17 15:52:21 2017, running configuration script [FreedomZTP.py]
ZTP, Fri Mar 17 15:58:28 2017, commit configuration
ZTP, Fri Mar 17 15:58:28 2017, ZTP succeed
ZTP, Fri Mar 17 15:58:28 2017, enable raslog
ZTP, Fri Mar 17 15:58:28 2017, ========== ZTP completed ==========
```

History

Release version	Command history
17s.1.00	This command was introduced.

diag burninerrclear

Clears the error logs, generated by system-verification failures, that are stored in nonvolatile memory.

Syntax

diag burninerrclear

Command Default

No test is executed.

Modes

Offline diagnostic mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

> ATTENTION
> Do not abort testing. This test must be allowed to run to completion.

To check the logs and error messages that are generated during system verification, use the following commands:

show diag burninerrshow

show diag burninstatus

Examples

The following example shows the output of this test.

```
diag<~>#  diag burninerrclear
% Info: This test should be run to completion. Please do not abort while it is executing.
Running burninerrclear...
clear following:
date: Thu Feb 17 15:30:57 UTC 2000
burninerr on round 1:
28:port loopback test on port 1 FAILED
30:port loopback test on port 2 FAILED
32:port loopback test on port 3 FAILED
34:port loopback test on port 4 FAILED

<---output truncated--->

128:port loopback test on port 51 FAILED
130:port loopback test on port 52 FAILED
132:port loopback test on port 53 FAILED
134:port loopback test on port 54 FAILED
135:<<port loopback test on All port FAILED>>
```

History

Release version	Command history
17s.1.00	This command was introduced.

diag portledtest

Executes portLedTest to test the LEDs on a single port or all ports on the device.

Syntax

diag portledtest [**port** { **all** | *number* }] [**off** | **on** }

Command Default

If no parameter is specified, the default setting is as follows: **diag portledtest port all on**

Parameters

port

Specifies a single port or all ports.

all

Specifies all ports.

number

Specifies a single port.

off

Turns off the LEDs.

on

Turns on the LEDs.

Modes

Offline diagnostic mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

ATTENTION

Do not abort testing. This test must be allowed to run to completion.

IMPORTANT

Remove or unplug all inserted transceiver or DAC modules prior to testing, to avoid LED errors.

It is recommended that you turn off all LEDs prior to making a visual check. Use the **reload** command to power cycle the device after testing.

The SLX 9240 has four LEDs per 40/100 gigabit port (ports 1 through 32).

The SLX 9140 has one LED per 10/25 gigabit port (ports 1 through 48), and four LEDs per 40 or 100 gigabit port (ports 49 through 54).

Examples

The following example tests all ports for the "off" condition.

```
diag<~>#  diag portledtest port all off
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portledtest...
0xFB800300: 0x23222120
0xFB800304: 0x27262524
0xFB800308: 0x2F2E2D2C
0xFB80030C: 0x2B2A2928
0xFB800310: 0x03020100
0xFB800314: 0x07060504
0xFB800318: 0x0B0A0908
0xFB80031C: 0x0F0E0D0C
0xFB800320: 0x13121110
0xFB800324: 0x17161514
0xFB800328: 0x1B1A1918
0xFB80032C: 0x1F1E1D1C
0xFB800330: 0x33323130
0xFB800334: 0x37363534
0xFB800338: 0x3B3A3938
0xFB80033C: 0x3F3E3D3C
0xFB800340: 0x5B5A5958
0xFB800344: 0x5F5E5D5C
0xFB800348: 0x57565554
0xFB80034C: 0x53525150
0xFB800350: 0x7F7E7D7C
0xFB800354: 0x7B7A7978
0xFB800358: 0x77767574
0xFB80035C: 0x73727170
0xFB800360: 0x6F6E6D6C
0xFB800364: 0x6B6A6968
0xFB800368: 0x67666564
0xFB80036C: 0x63626160
0xFB800370: 0x4B4A4948
0xFB800374: 0x4F4E4D4C
0xFB800378: 0x47464544
0xFB80037C: 0x43424140
-- Done --
[No LED on]
```

The following example tests port 1 for the "on" condition.

```
diag<~>#  diag portledtest port 1 on
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portledtest...
-- Done --
loopback on port 1
Warning: After performing this visual check, please PWR CYC this unit.
PWR-CYC Cmd : reload
```

History

Release version	Command history
17s.1.00	This command was introduced.

diag portloopbacktest

Executes portLoopbackTest to test a single port or all ports on the device.

Syntax

diag portloopbacktest [**port** { **all** | *number* } [**lbmode** { **0** | **1** }] [**nframes** *number*] [**spdmode** { **high** | **low** }]]

Command Default

The default settings are as shown in Parameters.

Parameters

port

Specifies a single port or all ports.

all

Specifies all ports. This is the default.

number

Specifies a single port.

lbmode

Specifies loopback test mode.

0

Tests the internal looback for inner Serializer/Deserializer (SerDes) lanes. This is the default.

1

Tests the external loopback for a single loopback module.

nframes *number*

Specifies the number of frames to be sent or received. Range is from 100 through 1000. The default is 100

spdmode

Specifies the port speed. Values for **high** and **low** are assigned according to the port and platform type.

high

Specifies 100 G mode for ports 1 through 32 on the SLX 9240. Specifies 25 G mode for ports 1 through 48 and 100 G mode for ports 49 through 54 on the SLX 9140. This is the default.

low

Specifies 40 G mode for ports 1 through 32 on the SLX 9240. Specifies 10 G mode for ports 1 through 48 and 40 G mode for ports 49 through 54 on the SLX 9140.

Modes

Offline diagnostic mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

ATTENTION

Do not abort testing. This test must be allowed to run to completion.

NOTE

For external loopback testing (**lbmode** = **1**), ensure that ports to be tested are connected with SFPs or loopback plugs.

Examples

The following example shows a default test on a SLX 9240 (internal loopback mode 0. all ports at 10 G).

```
diag<~># diag portloopbacktest
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
% Info: This test should be run to completion. Please do not abort while it is e
xecuting.
Running portloopbacktest...
Mode Data Rx-invert Tx-invert Injected-errors
Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 26 -prbsMode 31 -rxWidth 20 -txWidth 20 -divider 66
-loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0
0
Serdes PRBS Tests : PASS
port loopback test on port 1 PASSED
…
(xpShell):xpdiags)serdes_prbs_test 0 120 -prbsMode 31 -rxWidth 20 -txWidth 20 -divider 66
 -loopback ILB -tune 0 -duration 3

ILB SERDES_TX_DATA_SEL_PRBS31 false false 0
0
Serdes PRBS Tests : PASS
port loopback test on port 32 PASSED
<<port loopback test on All port PASSED>>
```

The following example shows a test on a SLX 9240 with loopback mode 1 and all ports at 40 G.

```
diag<~>#  diag portloopbacktest lbmode 1 spdmode 40
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 1 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 2 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 3 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 4 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 5 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 6 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 7 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 8 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 9 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 10 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 11 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 12 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 13 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 14 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 15 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 16 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 17 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 18 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 19 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 20 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 21 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 22 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 23 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 24 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 25 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 26 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 27 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 28 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 29 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 30 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 31 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 32 PASSED
<<port loopback test on All port PASSED>>
```

The following example tests a SLX 9240 with loopback mode 0 (the default) and all ports at 100 G.

```
diag<~># diag portloopbacktest spdmode 100
Mode Data Rx-invert Tx-invert Injected-errors
Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 26 -prbsMode 31 -rxWidth 20 -txWidth 20 -divider 66
 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0
0
Serdes PRBS Tests : PASS
port loopback test on port 1 PASSED
…
(xpShell):xpdiags)serdes_prbs_test 0 120 -prbsMode 31 -rxWidth 20 -txWidth 20 -divider 66
 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0
0
Serdes PRBS Tests : PASS
port loopback test on port 32 PASSED
<<port loopback test on All port PASSED>>
```

The following example tests a SLX 9240with a single port at 10 G (the default)

```
diag<~># diag portloopbacktest port 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Mode Data Rx-invert Tx-invert Injected-errors
Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 26 -prbsMode 31 -rxWidth 20 -txWidth 20 -di
vider 66 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- ---------------
-------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0
0
Serdes PRBS Tests : PASS
port loopback test on port 1 PASSED
```

The following example tests a SLX 9240 with loopback mode 1 and all ports at 10 G (the default)

```
diag<~>#  diag portloopbacktest lbmode 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 1 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 2 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 3 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 4 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 5 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 6 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 7 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 8 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 9 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 10 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 11 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 12 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 13 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 14 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 15 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 16 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 17 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 18 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 19 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 20 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 21 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 22 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 23 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 24 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 25 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 26 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 27 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=0
port loopback test on port 28 FAILED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 29 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 30 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 31 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=0
port loopback test on port 32 FAILED
<<port loopback test on All port FAILED>>
```

The following example tests a SLX 9240 on port 27 with loopback mode 1 and a default speed of 25 G.

```
diag<~># diag portloopbacktest port 27 lbmode 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_4X25GB' link 'Up', Rx=100
port loopback test on port 27 PASSED
```

The following example tests a SLX 9140 in loopback mode 0 with all ports at 25 G.

```
diag<~># diag portloopbacktest spdmode 25
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Mode Data Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 26 -prbsMode 31 -rxWidth 20 -txWidth 20 -divider 66
 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0

Serdes PRBS Tests : PASS
port loopback test on port 1 PASSED
…
(xpShell):xpdiags)serdes_prbs_test 0 108 -prbsMode 31 -rxWidth 20 -txWidth 20 -divider 66
 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0
Serdes PRBS Tests : PASS
port loopback test on port 54 PASSED
<<port loopback test on All port PASSED>>
```

The following example tests a SLX 9140 with loopback mode 0 and ports 49 through 54 at 100 G.

```
diag<~>#  diag portloopbacktest port 49,50,51,52,53,54 spdmode 100
Warning. Remove old log files du to log file space limit(10M)
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Mode Data Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 132 -prbsMode 31 -rxWidth 40 -txWidth 40 -divider
 165 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0
Serdes PRBS Tests : PASS
port loopback test on port 49 PASSED
Mode Data Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 124 -prbsMode 31 -rxWidth 40 -txWidth 40 -divider
165 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0
Serdes PRBS Tests : PASS
port loopback test on port 50 PASSED
Mode Data Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 100 -prbsMode 31 -rxWidth 40 -txWidth 40 -divider
165 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- ---------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0
Serdes PRBS Tests : PASS
port loopback test on port 51 PASSED
Mode Data Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 92 -prbsMode 31 -rxWidth 40 -txWidth 40 -divider
 165 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0
Serdes PRBS Tests : PASS
port loopback test on port 52 PASSED
Mode Data Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 116 -prbsMode 31 -rxWidth 40 -txWidth 40 -divider
165 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0
Serdes PRBS Tests : PASS
port loopback test on port 53 PASSED
Mode Data Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 108 -prbsMode 31 -rxWidth 40 -txWidth 40 -divider
165 -loopback ILB -tune 0 -duration 3
---------- ------------------------ --------- --------- --------------- -------------
ILB SERDES_TX_DATA_SEL_PRBS31 false false 0 0
Serdes PRBS Tests : PASS
port loopback test on port 54 PASSED
<<port loopback test on All port PASSED>>
```

The following example tests a SLX 9140 in loopback mode 1 for ports 49 through 54 at 100 G. (Ranging is currently not supported.)

```
diag<~>#  diag portloopbacktest port 49,50,51,52,53,54 spdmode 100 lbmode 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 49 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 50 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 51 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 52 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 53 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 54 PASSED
<<port loopback test on All port PASSED>>
```

The following example tests a SLX 9140 in loopback mode 0 on port 3, with port speed set to high and the number of frames set to 200.

```
diag<~>#diag portloopbacktest port 3 lbmode 0 spdmode hi nframes 200
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
      Mode                          Data    Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 28 -prbsMode 31 -rxWidth 40 -txWidth 40 -divider 165 -loopback ILB
-tune 0  -duration 3
----------      -------------------------    --------- --------- --------------- -------------
       ILB      SERDES_TX_DATA_SEL_PRBS31        false     false               0             0
Serdes PRBS Tests : PASS
port loopback test on port 3 PASSED
```

The following example tests a SLX 9140 in loopback mode 0 on port 3, with port speed set to low.

```
diag<~>#diag portloopbacktest port 30 lbmode 0 spdmode low
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
      Mode                          Data    Rx-invert Tx-invert Injected-errors Actual-Errors
(xpShell):xpdiags)serdes_prbs_test 0 61 -prbsMode 31 -rxWidth 20 -txWidth 20 -divider 66 -loopback ILB -
tune 0  -duration 3
----------      -------------------------    --------- --------- --------------- -------------
       ILB      SERDES_TX_DATA_SEL_PRBS31        false     false               0             0
Serdes PRBS Tests : PASS
port loopback test on port 30 PASSED
```

The following example tests a SLX 9140 on port 22, with loopback mode set to 1 and port speed set to low.

```
diag<~>#diag portloopbacktest port 22 lbmode 1 spdmode low
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_4X10GB' link 'Down', Rx=0
port loopback test on port 22 FAILED
```

The following example tests a SLX 9140 on ports 49 through 54, with loopback mode set to 1 and port speed set to low.

```
diag<~># diag portloopbacktest port 49,50,51,52,53,54 spdmode low lbmode 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 49 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 50 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 51 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 52 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 53 PASSED
Port type='MAC_MODE_1X40GB' link 'Up', Rx=100
port loopback test on port 54 PASSED
<<port loopback test on All port PASSED>>
Warning: After performing this test, please power-cycle the switch with reload command.
```

The following example tests a SLX 9140 on ports 49 through 54, with loopback mode set to 1 and port speed set to high.

```
diag<~>#  diag portloopbacktest port 49,50,51,52,53,54 spdmode hi lbmode 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 49 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 50 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 51 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 52 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 53 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 54 PASSED
<<port loopback test on All port PASSED>>
```

The following example tests a SLX 9240 on ports 49 through 54, with loopback mode set to 1 and port speed set to high.

```
diag<~>#  diag portloopbacktest port 49,50,51,52,53,54 spdmode hi lbmode 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Warning: Please insert single loopback modules into Ethernet ports prior to this test.
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 49 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 50 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 51 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 52 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 53 PASSED
Port type='MAC_MODE_1X100GB' link 'Up', Rx=100
port loopback test on port 54 PASSED
<<port loopback test on All port PASSED>>
```

History

Release version	Command history
17s.1.00	This command was introduced.

diag setcycle

Specifies the parameters for the system-verification test suite.

Syntax

diag setcycle { **default** | [**lbmode** { **0** | **1** } [**num_of_runs** *number*] [**pled_passes** *number*] [**tbr_passes** *number*] [**plb_nframes** *number*] }

Command Default

At least one parameter is expected.

Parameters

default
Restores default parameters for the next system-verification test.

lbmode
Specifies the loopback test mode.

0
Tests the internal looback for inner Serializer/Deserializer (SerDes) lanes. This is the default.

1
Tests the external looback for a single loopback modules.

num_of_runs *number*
Specifies the number of verification passes. Range is 1 through 25. The default is 1.

pled_passes *number*
Specifies the number of portLedTest passes. Range is 1 through 10. The default is 1.

tbr_passes *number*
Specifies the number of turboRamTest passes. Range is 1 through 10. The default is 1.

plb_nframes *number*
Specifies the number of portLoopbackTest frames at the default speed. The default number of frames is 100.

Modes

Offline diagnostic mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

Use the **show diag setcycle** command to confirm the results of this command.

Examples

To set the parameters to defaults for the next system-verification test to be run:

```
diag<~>#  diag setcycle default
% Info: This test should be run to completion. Please do not abort while it is executing.
Running setcycle...
DEFAULT - KEYWORD : COMMENT
0 - lb_mode : Limits -lb_mode of tests
1 - number_of_runs : number of passes of verify replacing 3 with default 1
1 - pled_passes : portledtest number of passes
1 - tbr_passes : turboramtest number of passes
100 - plb_nframes : portloopbacktest number of frames default speed
OFF-LINE DIAG SW SPEC V1.8 RELEASED DATE: FEB 08, 2017
ACCTON CONFIDENTIAL 2 6 CEDAR&FREEDOM
Committing changes to configuration
```

To set the loopback mode for the next system-verification test to be run to the nondefault setting:

```
diag<~>#  diag setcycle lb_mode 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running setcycle...
Setting lb_mode to 1.
Committing changes to configuration
```

To set the number of runs to 3:

```
diag<~>#  diag setcycle num_of_runs 3
% Info: This test should be run to completion. Please do not abort while it is executing.
Running setcycle...
Setting num_of_runs to 3.
Committing changes to configuration
```

History

Release version	Command history
17s.1.00	This command was introduced.

diag systemverification

Executes a system-verification test suite.

Syntax

diag systemverification

Command Default

No parameters are used.

Modes

Offline diagnostics mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

This is an "all-in-one" test for quick system checks. The tests are based on the parameters set by the **diag setcycle** command. Tests include turboRamTest, portLedTest, and portLoopBackTest. Tests may take a while time to complete.

For loopback testing, only the default speed is supported.

ATTENTION
Do not abort testing. This test must be allowed to run to completion. After this test completes, you must power-cycle the switch by means of the **reload** command before running additional offline diagnostic tests.

NOTE
For external loopback testing (**lbmode** = **1**), ensure that ports to be tested are connected with SFPs or loopback plugs.

Examples

The following example illustrates the execution of this test.

```
diag<~># diag systemverification
% Info: This test should be run to completion. Please do not abort while it is executing.
Running systemverification...

====================
date: Thu Feb 17 14:57:12 UTC 2000
systemverification on round 1
% Info: This test should be run to completion. Please do not abort while it is executing.
Running turboramtest...
loop#1: PASS
memt -s 500 : PASSED
loop#1: PASS
memt -s 300 -a 1: PASSED
memtester.sh : PASSED
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portledtest...
0xFB800300: 0xFFFFFFFF
0xFB800304: 0x14FFFFFF
0xFB800308: 0x13121110
0xFB80030C: 0x18171615

<---output truncated--->

-- Done --
xp80FirmwareB0-2016-0502-1906.bin loaded
[All LED on]
-- Done --
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 1 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 2 PASSED

<---output truncated--->

port loopback test on port 54 PASSED
<<port loopback test on All port PASSED>>
% Info: This test should be run to completion. Please do not abort while it is executing.
Running prbstest...
Warning: PRBS test isn't available yet.
systemverification on round 1: No error messages
Warning: After performing this system check, please PWR CYC this unit.
PWR-CYC Cmd : reload
```

History

Release version	Command history
17s.1.00	This command was introduced.

diag turboramtest

Executes turboRamTest on the device to check DDR SDRAM.

Syntax

diag turboramtest [**passcnt** *count*]

Command Default

If **passcnt** is not specified, only one test is executed.

Parameters

passcnt *count*

Specifies the number of test loops to be run. Range is 1 though 10.

Modes

Privileged EXEC mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

ATTENTION
Do not abort testing. This test must be allowed to run to completion.

If **passnct** is not specified, only one test is executed (the default).

Examples

The following example executes the default number of test loops (1).

```
device# diag turboramtest
% Info: This test should be run to completion. Please do not abort while it is executing.
Running turboramtest...
loop#1: PASS
memt -s 500 : PASSED
loop#1: PASS
memt -s 300 -a 1: PASSED
memtester.sh : PASSED
```

The following example executes two test loops.

```
device# diag turboramtest passcnt 2
OFF-LINE DIAG SW SPEC V1.8 RELEASED DATE: FEB 08, 2017
ACCTON CONFIDENTIAL 1 1 CEDAR&FREEDOM
% Info: This test should be run to completion. Please do not abort while it is executing.
Running turboramtest...
turboRamTest on round 1
loop#1: PASS
memt -s 500 : PASSED
loop#1: PASS
memt -s 300 -a 1: PASSED
memtester.sh : PASSED
turboRamTest on round 2
loop#1: PASS
memt -s 500 : PASSED
loop#1: PASS
memt -s 300 -a 1: PASSED
memtester.sh : PASSED
```

History

Release version	Command history
17s.1.00	This command was introduced.

dir

Lists the contents of the device flash memory.

Syntax

dir

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

The following example lists the contents of the flash memory.

```
device# dir
total 4136
drwxr-xr-x   2 root     root         4096 Feb 13 08:18 .
drwxr-xr-x   3 root     root         4096 Mar 31  2000 ..
-rw-r--r--   1 root     root        12946 Jan  9 16:35 bfd-mib.cfg
-rw-r--r--   1 root     root        12738 Dec 16 12:51 default_config
-rw-r--r--   1 root     sys           495 Jan 30 04:12 defaultconfig.cluster
-rw-r--r--   1 root     root          446 Jan 31 15:08 defaultconfig.standalone
-rw-r--r--   1 root     root        49534 Jan 24 16:13 ipv4_64-way-ecmp_unid.cfg
-rw-r--r--   1 root     root       187126 Dec  7 13:54 ipv4_bfd_unid_200ospf_250
bgp.cfg
-rw-r--r--   1 root     root       132842 Dec  8 17:03 ipv4_bfd_unid_250static.c
fg
-rw-r--r--   1 root     root       105355 Jan 27 15:17 ipv4_bgp-peer-group-scale
-250_unid.cfg
-rw-r--r--   1 root     root        85734 Jan 25 15:43 ipv4_bgp-ribin-ribout-sca
le-3.2M-9.6M_unid.cfg
-rw-r--r--   1 root     root        85779 Jan 26 11:33 ipv4_bgp-ribin-ribout-sca
le-320k-3.8M_unid.cfg
-rw-r--r--   1 root     root        85754 Jan 26 14:38 ipv4_bgp-ribin-ribout-sca
le-320k-320k_unid.cfg
-rw-r--r--   1 root     root        49460 Jan 20 12:22 ipv4_ebgp-scale-256_unid.
cfg
-rw-r--r--   1 root     root        49460 Jan 21 19:25 ipv4_hw-route-scale-48k_u
nid.cfg
-rw-r--r--   1 root     root        97274 Dec 23 11:32 ipv4_static-128-vrf_unid.
cfg
-rw-r--r--   1 root     root       149596 Dec 21 14:56 ipv4_static-64-way-ecmp_u
nid.cfg
-rw-r--r--   1 root     root       288612 Dec 13 11:50 ipv4_unid_1kvrf.cfg
-rw-r--r--   1 root     root       401259 Dec 16 12:34 ipv4_unid_static_route_sc
ale_12k
-rw-r--r--   1 root     root        23583 Dec 19 19:39 ipv6_64-way-ecmp_unid.cfg
-rw-r--r--   1 root     root       173679 Dec  8 14:47 ipv6_bfd_unid_200ospf.cfg
-rw-r--r--   1 root     root       173560 Dec  8 14:31 ipv6_bfd_unid_250bgp.cfg
-rw-r--r--   1 root     root       134777 Dec 14 15:07 ipv6_bfd_unid_250static.c
fg
-rw-r--r--   1 root     root        58256 Jan 11 11:48 ipv6_bgp-64-way-ecmp_unid
.cfg
-rw-r--r--   1 root     root        31238 Jan 11 14:45 ipv6_bgp-ribin-10k-ribout
-100k_unid.cfg
-rw-r--r--   1 root     root        36536 Jan 11 16:45 ipv6_bgp-ribin-32k-ribout
-1M_unid.cfg
-rw-r--r--   1 root     root        58187 Jan 10 17:14 ipv6_bgp_unid_256.cfg
-rw-r--r--   1 root     root       217061 Jan 12 15:27 ipv6_intf-scale-2k_unid.c
fg
-rw-r--r--   1 root     root       346540 Jan 17 16:22 ipv6_ipv6-addr-scale_unid
.cfg
-rw-r--r--   1 root     root       232616 Dec  7 16:56 ipv6_ospf_bgp_bfd_250.cfg
-rw-r--r--   1 root     root        13013 Dec 19 17:20 ipv6_rib_fib_unid_4k.cfg
-rw-r--r--   1 root     root       227795 Jan 13 14:55 ipv6_sec-addr-scale-255_u
nid.cfg
-rw-r--r--   1 root     root        60434 Jan  3 17:43 ipv6_static-128-vrf_unid.
cfg
-rw-r--r--   1 root     root        61359 Dec 21 15:43 ipv6_static-64-way-ecmp_u
nid.cfg
-rw-r--r--   1 root     root       129253 Dec 16 16:04 ipv6_unid_static_route_sc
ale_3k
-rw-r--r--   1 root     root       279380 Jan 19 15:25 ipv6_ve-vrf-scale_unid.cf
g
-rw-r--r--   1 root     root          446 Feb  8 14:38 startup-config

16282714112 bytes total (9539092480  bytes free)
```

History

Release version	Command history
17s.1.00	This command was introduced.

disable (LLDP)

Disables Link Layer Discovery Protocol (LLDP) globally without changing any other aspect of the LLDP configuration.

Syntax

disable

no disable

Command Default

LLDP is enabled globally by default.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter the **no disable** to re-enable LLDP.

Examples

The following example disables LLDP.

```
device# configure terminal
device(config)# protocol lldp
device(config-lldp)# disable
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

The **no** form of the command restores the defaults.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

distance (OSPF)

Configures an administrative distance value for OSPFv2 and OSPFv3 routes.

Syntax

distance { **external** | **inter-area** | **intra-area** | **route-map** } *distance*

no distance

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.

route-map
Sets the distance based on route maps 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 restores the defaults.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

domain

In PTP configuration mode, specifies a Precision Time Protocol clock domain.

Syntax

domain *domain_id*

no domain

Command Default

See the Usage Guidelines.

Parameters

domain_id

Specifies a nondefault PTP clock domain. Range is from 0 through 255. The default is 0. See the Usage Guidelines.

Modes

PTP configuration mode

Usage Guidelines

Only a single domain can be specified, and only clocks in the same domain can communicate with each other.

Use the **no** form of this command to revert to domain ID 0.

Examples

To specify a nondefault clock domain:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# domain 1
```

To remove a nondefault clock domain, leaving domain 0:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# no domain
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x authentication

Enables 802.1x authentication on a port.

Syntax

dot1x authentication

no dot1x authentication

Command Default

802.1x authentication is disabled.

Modes

Interface configuration mode

Usage Guidelines

NOTE
To activate authentication on an 802.1x-enabled interface, port control must be configured. You can configure port control by using the **dot1x port-control auto** command in interface configuration mode.

Use the **no** form of the command to disable 802.1x authentication on the port and remove the configuration from 802.1x management configuration.

Examples

The following example enables 802.1x authentication on Ethernet port 0/1.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x authentication
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x enable

Enables 802.1X port authentication globally.

Syntax

dot1x enable

Command Default

802.1x port authentication is not enabled.

Modes

Global configuration mode

Usage Guidelines

NOTE
802.1x port authentication is not supported by Link Aggregation Group (LAG) or interfaces that participate in a LAG.

Examples

The following example enables 802.1X authentication globally on all interfaces.

```
device# configure terminal
device(config)# dot1x enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x port-control

Controls the port authorization state 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

By default, the port state is authorized.

Parameters

auto

Allows a client on an 802.1X-enabled interface to negotiate authentication. The port is placed in the unauthorized state until authentication takes places between the client and the authentication server. When authentication is enabled by using the **dot1x authentication** command and the client is authenticated by the authentication server, the port state changes to the authorized. The controlled port remains in the authorized state until the client logs off.

force-authorized

Unconditionally places the controlled port in the authorized state, allowing all traffic to pass between the client and the authenticator. This also allows connection from multiple clients.

force-unauthorized

Unconditionally places the controlled port in the unauthorized state, denying any traffic to pass between the client and the authenticator.

Modes

Interface configuration mode

Usage Guidelines

Before activating authentication by specifying the **auto** option, you must remove any static ACLs or static VLANs configured on the port.

802.1x port authentication is not supported by Link Aggregation Group (LAG) 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 unconditionally place the port in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x port-control auto
```

The following example configures the interface to unconditionally place the controlled port in the authorized state.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x port-control force-authorized
```

The following example configures the interface to unconditionally place the controlled port in the unauthorized state.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x port-control force-unauthorized
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x quiet-period

Configures the interval that the device remains idle between a failed authentication attempt and a subsequent 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 a failed authentication attempt and a subsequent reauthentication attempt. Valid values range from 1 through 65535 seconds.

Modes

Interface configuration mode

Usage Guidelines

Changing the quiet-period interval 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 shows how to set the quiet time to 200 seconds.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x quiet-period 200
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x reauthenticate

Enables 802.1X reauthentication on a specific interface.

Syntax

dot1x reauthenticate interface ethernet *slot/port*

Parameters

interface ethernet *slot/port*

Specifies enabling reauthentication on an Ethernet interface. The interface is specified in slot and port number format; when the device does not contain slots, the slot number must be 0.

Modes

Privileged EXEC mode

Examples

The following example enables reauthentication of a client connected to Ethernet interface 0/1.

```
device# dot1x reauthenticate interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x reauthentication

Enables periodic reauthentication of clients connected to an 802.1X-enabled interface.

Syntax

dot1x reauthentication

no dot1x reauthentication

Command Default

Periodic reauthentication is disabled.

Modes

Interface configuration mode

Usage Guidelines

When periodic reauthentication is enabled by using the **dot1x reauthentication** command, the device reauthenticates clients every 3,600 seconds by default.

The reauthentication interval is configurable using the **dot1x timeout** command. The reauthentication interval configured by using the **dot1x timeout** command takes precedence.

The **no** form of the command disables periodic reauthentication.

Examples

The following example enables 802.1x reauthentication of clients connected to Ethernet interface 0/1.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x reauthentication
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x reauthMax

Configures 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

By default, a port makes two 802.1x reauthentication attempts before changing to the unauthorized state,

Parameters

number

Specifies the maximum number of reauthentication attempts before the port goes to the unauthorized state. The range is 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 for Ethernet interface 0/1.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x reauthMax 5
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x test eapol-capable

Executes the 802.1x readiness check on a specific interface.

Syntax

dot1x test eapol-capable interface ethernet *slot/port*

Parameters

interface ethernet *slot/port*

Specifies an Ethernet inteface for the readiness check. The interface is specified in slot and port number format; when the device does not contain slots, the slot number must be 0.

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 command 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 by using the **dot1x port-control force-unauthorized** command.

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. It is not possible to do an 802.1x readiness check for all interfaces at once.

Examples

The following example configures readiness check on an Ethernet interface (0/1), to determine if the devices connected to the port are 802.1x-capable.

```
device# dot1x test eapol-capable interface ethernet 0/1

2016/07/18-00:49:03, [DOT1-1012], 5006, M2 | Active | DCE, INFO, sw0, DOT1X_PORT_EAPOL_CAPABLE:
Peer connected to port Ethernet 0/1 is EAPOL capable.
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x test timeout

Configures the timeout period for the 802.1X readiness test.

Syntax

dot1x test timeout *timeout*

Command Default

The default timeout period for the 802.1X readiness test is 10 seconds.

Parameters

timeout

Specifies the readiness test timeout period in seconds. The valid range is from 1 through 65535.

Modes

Global configuration mode

Examples

The following example shows how to set the timeout period for the 802.1X readiness test to 30 seconds.

```
device# configure terminal
device(config)# dot1x test timeout 30
```

History

Release version	Command history
17s.1.00	This command was introduced.

dot1x timeout

Configures parameters for the 802.1x timeout period for client reauthentication and Extensible Authentication Protocol (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

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 an alternate 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. The valid range is from 1 through 65535 seconds. The default value is 30 seconds.

By default, when the device does not receive an EAP response or identity frame from a client, the device waits 30 seconds, then retransmits the EAP request or identity frame. You can optionally change the amount of time the device waits before retransmitting the EAP request or identity frame to the client. When the client does not send back an EAP response or identity frame within 60 seconds, the device transmits another EAP request or identity frame.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables the 802.1x timeout period configuration.

Examples

The following example sets to 25 seconds, the time between reauthorization attempts on Ethernet interface 0/1.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x timeout re-authperiod 25
```

The following example sets to 45 seconds, the switch-to-client retransmission time for the EAP request frame on Ethernet interface 0/1.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x timeout supp-timeout 45
```

The following example sets to 34 seconds, the waiting period (before retransmitting the request) for a response to an EAP request or identity frame from the client on Ethernet interface 0/1.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# dot1x timeout tx-period 34
```

History

Release version	Command history
17s.1.00	This command was introduced.

duplicate-mac-timer (EVPN)

Configures a duplicate MAC detection timer for the detection of continuous MAC moves for an Ethernet VPN (EVPN) instance.

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 myinstance
device(config-evpn-myinstance)# 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 myinstance
device(config-evpn-myinstance)# no duplicate-mac-timer
```

History

Release version	Command history
17s.1.01	This command was introduced.

Commands E - F

efa debug clear-config

Clears the EFA configuration from the device.

Syntax

efa debug clear-config [**--device** *string* | **--help** | **--password** *string* | **--username** *string*]

Command Default

This command has no defaults.

Parameters

--device *string*
Specifies a comma-separated list of device IP addresses or hostnames.

--help
Provides help for command options.

--password *string*
Clears the password for a comma-separated list of device IP addresses or hostnames.

--username *string*
Clears the username for a comma-separated list of device IP addresses or hostnames.

Modes

TPVM configuration mode

Examples

This example clears all EFA configured parameters for three devices.

```
$ efa debug clear-config --device 10.25.225.160,10.25.225.161,10.25.225.162
```

History

Release version	Command history
17s.1.02b	This command was introduced.

efa deploy

Deploys the EFA application.

Syntax

efa deploy [**--help** | **--password** *string* | **--username** *string*]

Command Default

This command has no defaults.

Parameters

--help
Provides help for command options.

--password *string*
Specifies a password.

--username *string*
Specifies a username.

Modes

TPVM configuration mode

Usage Guidelines

This command is executed in TPVM configuration mode on one of the SLX switches within the fabric.

ATTENTION
This command causes TPVM to reboot.

The username and password are optional. The defaults "root" and "fibranne" are used if not specified.

Examples

This example deploys EFA.

```
$ efa deploy username root password fibranne
```

History

Release version	Command history
17s.1.02b	This command was introduced.

efa device credentials update

Updates the credentials of existing devices in an IP Fabric. This should be used before deconfiguring or refreshing a device if the device credentials have been changed.

Syntax

efa device credentials update [**--device** *string* | **--help** | **--password** *string*| **--username** *string*]

Command Default

This command has no defaults.

Parameters

--device *string*
Specifies a comma-separated list of device IP addresses or hostnames.

--help
Provides help for command options.

--password *string*
Specifies the password for a comma-separated list of device IP addresses or hostnames.

--username *string*
Specifies the username for a comma-separated list of device IP addresses or hostnames.

Modes

TPVM configuration mode

Usage Guidelines

The keywords are required. Otherwise an error is thrown, as shown below.

```
Error: Required flag(s) "device", "password", "username" have/has not been set
```

Examples

This example updates credentials for all devices in the fabric.

```
$ efa device credentials updatedevice 10.2.3.4 password mypassword username myusername
```

History

Release version	Command history
17s.1.02b	This command was introduced.

efa execution show

Displays the status and execution details of previous CLI or REST executions of the application.

Syntax

efa execution show [**--id** *string*] | **limit** *int32* [**--status** [**all** | **failed** | **succeeded**]

Parameters

--id *string*

Filters execution according to the execution ID.

--limit *int32*

Limits the number of executions to be listed, where *int32* is an unsigned integer (default is 10).

--status

Specifies whether the status of execution shows failed or succeeded.

all

Specifies all executions. This is the default, returning both succeeded and failed executions.

failed

Specifies failed executions.

succeeded

Specifies succeded executions.

Modes

TPVM configuration mode

Usage Guidelines

Examples

This is example output without any arguments.

```
$ efa execution show
+--------------------------------------+---------------+----------------------+---------------------------
+--------------------------+
|                  ID                  |    COMMAND    |        STATUS        |        START TIME
|         END TIME          |
+--------------------------------------+---------------+----------------------+---------------------------
+--------------------------+
| 173c0fa4-8cc5-4beb-bf15-ccf900071c5b | fabric show   | Completed(54.2014ms) | 2018-01-25T10:36:46+05:30 |
2018-01-25T10:36:46+05:30 |

| 68fec530-b7da-4606-a7a9-b4648019dbfe | configure add | Failed(15.1241363s)  | 2018-01-22T14:29:09+05:30 |
2018-01-22T14:29:25+05:30 |

+--------------------------------------+---------------+----------------------+---------------------------
+--------------------------+
```

Output field	Description
ID	Execution ID of the CLI request
Command	CLI command that is executed
STATUS	Completed or Failed status of the command
START TIME	Time when the command is received
END TIME	Time when the command execution is completed

This is example output with an execution ID specified.

```
efa execution show --id 68fec530-b7da-4606-a7a9-b4648019dbfe

id: 68fec530-b7da-4606-a7a9-b4648019dbfe
command: configure add
parameters: {spines: leaves:["10.24.73.204","1.24.73.205"]}
status: Failed
duration: 768ms
errors: "No Spine devices"
```

Output field	Description
ID	Execution ID of the CLI request
Logs	Logs for the given execution ID (error logs are displayed by default)

History

The **efa execution show** command displays the following information.

Release version	Command history
17s.1.02b	This command was introduced.

efa fabric configure

Registers switches and their roles with a default IP Fabric, for both Clos and non-Clos topologies.

Syntax

efa fabric configure { **--leaf** *list-of-leaf-ips* **--spine** *list-of-spine-ips* } [**--persist** | **--force**] [**--username** *string* **--password** *string*]

efa fabric configure { **--rack** *pair-of-rack-ips* } [**--persist** | **--force**] [**--username** *string* **--password** *string*]

Command Default

No devices are added, deleted, or configured by default. See the Usage Guidelines.

Parameters

--leaf *list-of-leaf-ips*
: Specifies a comma-separated list of leaf management IP addresses in an IP Clos topology.

--rack *pair-of-rack-ips*
: Specifies a comma-separated list of rack IP addresses in a non-Clos topology, taking a pair of IP addresses of the nodes that form an MCT pair.

--spine *list-of-spine-ips*
: Specifies a comma-separated list of spine management IP addresses in an IP Clos topology.

--force
: Replaces any conflicting configurations needed for fabric formation on the switch with the one inferred by the application. This involves overwriting the following: ASNs based on a fabric template; IP addresses of physical, loopback, and VE interfaces; overlay gateway configuration; EVPN instance; and MCT cluster configuration.

--persist
: Executes **copy running-config startup-config** on all leaf and spine devices.

username *string*
: Specifies a username. The default credentials used by the application are "admin" and "password". This option can be used to override the default credentials. The credentials apply for all devices that are provided as part of the command. In case the devices have different credentials, they can be added by means of a separate command.

password *string*
: Specifies a password.

Modes

TPVM configuration mode

Usage Guidelines

This command is executed in TPVM configuration mode on one of the SLX switches within the fabric.

Up to four rack pairs are supported in a non-Clos topology.

Examples

This IP Clos example adds leaf and spine nodes to the fabric and resolves conflicting configurations on the switch.

```
$ efa fabric configure --leaf 10.24.73.203,10.24.73.204,10.24.73.205,10.24.73.206 --spine
10.24.73.201,10.24.73.202  --username admin --password password --force
```

This IP Clos example adds more leaf nodes to the fabric.

```
$ efa fabric configure --leaf 10.24.73.207,10.24.73.208
```

This IP Clos example adds more spine nodes to the fabric.

```
$ efa fabric configure --spine 10.24.73.209,10.24.73.210
```

This non-Clos example configures a rack in the fabric and replaces conflicting configurations.

```
$ efa fabric configure --rack 10.24.73.203,10.24.73.204 -rack 10.24.73.205,10.24.73.206 --rack
10.24.73.201,10.24.73.202 --username admin --password password -force
```

This non-Clos example configures additional racks.

```
$ efa fabric configure --rack 10.24.73.207,10.24.73.208
```

History

Release version	Command history
17s.1.02b	This command was introduced.
18s.1.01a	This command was updated to support non-Clos topologies.

efa fabric deconfigure

Deletes switches from the IP Fabric, for both Clos and non-Clos topologies.

Syntax

efa fabric deconfigure { **--device** *list-of-device-ips* } [**--persist**] [**--username** *string* **--password** *string*]

efa fabric deconfigure { **--rack** *pair-of-rack-ips* } [**--persist**] [**--username** *string* **--password** *string*]

efa fabric deconfigure { **--no-device-cleanup** [**--username** *string* **--password** *string*]

Command Default

No devices are deleted by default.

Parameters

--device *list-of-device-ips*
Specifies a comma-separated ist of device IP addresses in an IP Clos topology.

--no-device-cleanup
Do not clean up the configurations on the devices. See the Usage Guidelines.

--rack *pair-of-rack-ips*
Specifies a comma-separated ist of rack IP addresses in a non-Clos topology.

--persist
Executes **copy running-config startup-config** on all leaf and spine devices.

username *string*
Specifies a username. The default credentials used by the application are "admin" and "password" . This option can be used to override the default credentials. The credentials apply for all devices that are provided as part of the command. In case the devices have different credentials, they can be added by means of a separate command.

password *string*
Specifies a password.

Modes

TPVM configuration mode

Usage Guidelines

This command is executed in TPVM configuration mode on one of the SLX switches within the fabric.

ATTENTION
Exercise the **--no-device-cleanup** option with caution. Use it only when configuration and deconfiguration commands are failing. This command can be used to clean up the devices from the database. No BGP or fabric link configurations are deleted from the neighboring switches.

Examples

This example deletes racks from the fabric and resolves conflicting configurations on the switch.

```
$ efa fabric deconfigure --rack 10.24.73.207,10.24.73.208
```

History

Release version	Command history
17s.1.02b	This command was introduced.
18s.1.01a	This command was updated to support non-Clos topologies.

efa fabric setting show

Displays the parameters of an IP Fabric, for both IP Clos and non-Clos topologies.

Syntax

efa fabric setting show [**--advanced**]

Parameters

--advanced

Displays advanced fabric parameters.

Modes

TPVM configuration mode

Command Output

This command is executed in TPVM configuration mode on one of the SLX switches within the fabric.

Examples

This is example output for basic parameters in an IP Clos topology.

```
$ efa fabric setting show
+---------------------------+-----------------+
|           NAME            |      VALUE      |
+---------------------------+-----------------+
| Fabric Name               | default         |
+---------------------------+-----------------+
| Link IP Range             | 10.10.10.0/23   |
+---------------------------+-----------------+
| Loopback IP Range         | 172.31.254.0/24 |
+---------------------------+-----------------+
| Loopback Port Number      | 1               |
+---------------------------+-----------------+
| VTEP Loopback Port Number | 2               |
+---------------------------+-----------------+
| Spine ASN Block           | 64512           |
+---------------------------+-----------------+
| Leaf ASN Block            | 65000-65534     |
+---------------------------+-----------------+
| P2P IP Type               | numbered        |
+---------------------------+-----------------+
| Fabric Type               | clos            |
+---------------------------+-----------------+
--- Time Elapsed: 2.9323ms ---
```

This is example output for basic parameters in a non-Clos topology.

```
$ efa fabric setting show
+---------------------------+-----------------------+
|           NAME            |         VALUE         |
+---------------------------+-----------------------+
| Fabric Name               | default               |
+---------------------------+-----------------------+
| Link IP Range             | 10.10.10.0/23         |
+---------------------------+-----------------------+
| Loopback IP Range         | 172.31.254.0/24       |
+---------------------------+-----------------------+
| Loopback Port Number      | 1                     |
+---------------------------+-----------------------+
| VTEP Loopback Port Number | 2                     |
+---------------------------+-----------------------+
| Rack ASN Block            | 4200000000-4200065534 |
+---------------------------+-----------------------+
| L3 Backup IP Range        | 10.30.30.0/24         |
+---------------------------+-----------------------+
| Fabric Type               | non-clos              |
+---------------------------+-----------------------+
--- Time Elapsed: 1.9894ms ---
```

This is example output for advanced parameters, showing rack peer group configurations for a non-Clos topology.

```
$ efa fabric setting show --advanced
+--------------------------------+-----------------------+
|              NAME              |         VALUE         |
+--------------------------------+-----------------------+
| Fabric Name                    | default               |
+--------------------------------+-----------------------+
| Link IP Range                  | 10.10.10.0/23         |
+--------------------------------+-----------------------+
| Loopback IP Range              | 172.31.254.0/24       |
+--------------------------------+-----------------------+
| Loopback Port Number           | 1                     |
+--------------------------------+-----------------------+
| VTEP Loopback Port Number      | 2                     |
+--------------------------------+-----------------------+
| Rack ASN Block                 | 4200000000-4200065534 |
+--------------------------------+-----------------------+
| L3 Backup IP Range             | 10.30.30.0/24         |
+--------------------------------+-----------------------+
| Fabric Type                    | non-clos              |
+--------------------------------+-----------------------+
| Any cast MAC                   | 0201.0101.0101        |
+--------------------------------+-----------------------+
| IPV6 Any cast MAC              | 0201.0101.0102        |
+--------------------------------+-----------------------+
| ARP Aging Timeout              | 300                   |
+--------------------------------+-----------------------+
| MAC Aging Timeout              | 1800                  |
+--------------------------------+-----------------------+
| MAC Aging Conversational       | 300                   |
| Timeout                        |                       |
+--------------------------------+-----------------------+
| MAC Move Limit                 | 20                    |
+--------------------------------+-----------------------+
| Duplicate MAC Timer            | 5                     |
+--------------------------------+-----------------------+
| Duplicate MAC Timer MAX Count  | 3                     |
+--------------------------------+-----------------------+
| BFD Enable                     | No                    |
+--------------------------------+-----------------------+
| BGP MultiHop                   | 4                     |
+--------------------------------+-----------------------+
| MaxPaths                       | 8                     |
+--------------------------------+-----------------------+
| AllowAsIn                      | 0                     |
+--------------------------------+-----------------------+
| MTU                            | 9216                  |
+--------------------------------+-----------------------+
| IPMTU                          | 9100                  |
+--------------------------------+-----------------------+
| Rack Peer EBGP Group           | underlay-ebgp-group   |
+--------------------------------+-----------------------+
| Rack Peer Overlay Evpn Group   | overlay-ebgp-group    |
+--------------------------------+-----------------------+
| MCT Link IP Range              | 10.20.20.0/24         |
+--------------------------------+-----------------------+
| MCT PortChannel                | 1024                  |
+--------------------------------+-----------------------+
| Routing MCT PortChannel        | 64                    |
+--------------------------------+-----------------------+
| Control Vlan                   | 4090                  |
+--------------------------------+-----------------------+
| Control VE                     | 4090                  |
+--------------------------------+-----------------------+
| VNI Auto Map                   | Yes                   |
+--------------------------------+-----------------------+
--- Time Elapsed: 2.957ms ---
```

History

Release version	Command history
17s.1.02b	This command was introduced.
18s.1.01a	This command was updated to support non-Clos topologies.

efa fabric setting update

Allows the user to modify the settings of an IP Fabric.

Syntax

efa fabric setting update {**--allow-as-in** *string* |**--anycast-mac-address** *string* |**--arp-aging-timeout** *string* |**--bfd-multiplier** *string* |**--bfd-rx** *string* |**--bfd-tx** *string* |**--bgp-multihop** *string* |**--configure-overlay-gateway** *string* } |**control-ve** *string*| **control-vlan** *string* |**--duplicate-mac-timer** *string* |**--duplicate-mac-timer-max-count** *string* |**--help** | **--ip-mtu** *string* |**--ipv6-anycast-mac-address** *value* |**--leaf-asn-block** *string* |**--leaf-peer-group** *string* |**--loopback-ip-range** *string* | --loopback-port-number *string* |**--mac-aging-conversation-timeout** *string* |**--mac-aging-timeout** *string* |**--mac-move-limit** *string* |**--max-paths** *string* | **--mct-port-channel** *string* |**--mctlink-ip-range** *string* |**--mtu** *string* |**--p2p-ip-type** *string* |**--p2p-link-range** *string* |**--spine-asn-block** *string* |**--spine-peer-group** *string* |**--vni-auto-map** *string* |**--vteploopback-port-number** *string* |**--l3-backup-ip-range***string* |**--rack-asn-block***string* |**--rack-peer-ebgp-group***string* |**--rack-peer-overlay-evpn-group***string* |**--fabric-type***string*}

Command Default

No command defaults apply.

Parameters

--allow-as-in *string*
Disables the AS_PATH check of the routes learned from the AS. Range is from 1 through 10.

--anycast-mac-address *string*
Specifies an IPv4 anycast MAC address in HHHH.HHHH.HHHH format.

--arp-aging-timeout *string*
Specifies how long an ARP entry stays in the cache. Range is from 60 through 100000 seconds.

--bfd-multiplier *string*
Specifies a multiplier for BFD detection time. Range is from 3 through 50.

--bfd-rx *string*
Specifies the BFD desired minimum receive interval in milliseconds. Range is from 50 through 30000.

--bfd-tx *string*
Specifies the BFD desired minimum transmit interval in milliseconds. Range is from 50 through 30000.

--bgp-multihop *string*
Specifies EBGP neighbors to allow when they are not on directly connected networks. Range is from 1 through 255.

--**configure-overlay-gateway** *string*
Specifies whether an overlay gateway is enabled or not. Options are "yes" or "no".

--control-ve *string*
Specifies a VLAN. Range is from 1 through 4090.

--control-vlan *string*
Specifies a VLAN. Range is from 1 through 4090.

--duplicate-mac-timer *string*
Specifies duplicate MAC timer.

--duplicate-mac-timer-max-count *string*
Specifies duplicate MAC timer max count.

--fabric-type
Specifies a fabric type. Options are "clos" and "non-clos".

--help
Specifies help for options for this command.

--ip-mtu *string*
Specifies an IPv4 or IPv6 MTU size in bytes for an SLX device. Range is from 1300 through 9194.

--ipv6-anycast-mac-address *string*
Specifies an IPv6 anycast MAC address in HHHH.HHHH.HHHH format.

--l3-backup-ip-range *string*
Specifies a range of Layer 3 backup IP addresses.

--leaf-asn-block *string*
Specifies a leaf ASN range, in comma-separated format.

--leaf-peer-group *string*
Specifies the name of a leaf peer group. Range is from 1 through 63 ASCII characters.

--loopback-ip-range *string*
Specifies a range of loopback IP addresses.

--loopback-port-number *string*
Specifies a loopback port number. Range is from 1 through 255.

--mac-aging-conversation-timeout *string*
Specifies the MAC conversational aging time in seconds. Range is from 60 through 100000. The default is 0.

--mac-aging-timeout *string*
Specifies the MAC aging time in seconds. Range is from 60 through 100000. The default is 0.

--mac-move-limit *string*
Specifies the MAC move detection limit. Range is from 5 through 500.

--max-paths *string*
Specifies the maximum number of paths for packet forwarding. Range is from 1 through 64.

--mct-port-channel *string*
Specifies a port-channel interface number. Range is from 1 through 1024.

--mctlink-ip-range *string*
Specifies a range of IP addresses.

--mtu *string*
Specifies the MTU size in bytes. Range is from 1548 through 9216.

--p2p-ip-type *string*
Specifies the IP type as numbered or unnumbered.

--rack-asn-block *string*
Specifies a rack ASN range, as a single AS or as comma-separated AS values.

--rack-peer-ebgp-group *string*
Specifies a rack peer EBGP group.

--rack-peer-overlay-evpn-group *string*
Specifies a rack peer overlay EVPN group.

--spine-asn-block *string*
Specifies a spine ASN range, as a single AS or as comma-separated AS values.

--spine-peer-group *string*
Specifies the name of a spine peer group. Range is from 1 through 63 ASCII characters.

--vni-auto-map *string*
Specifies whether VNI automapping used or not. Options are "yes" or "no".

--vtep-loopback-port-number *string*
Specifies a VTEP loopback port number. Range is from 1 through 255.

Modes

TPVM configuration mode

Usage Guidelines

This command is executed in TPVM configuration mode on one of the SLX switches within the fabric.

Examples

This example specifies a range of leaf switches.

```
$ efa fabric setting update --leaf_asn_block 65000-65534
```

This example specifies a range of IP addresses to be used for fabric links.

```
$ efa fabric setting update --link_ip_range 10.10.10.0/23
```

History

Release version	Command history
17s.1.02b	This command was introduced.
18s.1.01a	This command was updated to support non-Clos topologies.

efa fabric setting

Specifies whether an EFA IP fabric supports Clos or non-Clos networks.

efa fabric setting { **--fabric-type** { **clos** | **non-clos** }

Command Default

If not specified, the default (**clos**) supports IP Clos networks.

Parameters

--fabric-type
Specifies the IP Fabric as Clos or non-Clos.

clos
Supports an IP Clos network.

non-clos
Supports a non-Clos network.

Modes

TPVM configuration mode

Usage Guidelines

This command is executed in TPVM configuration mode on one of the SLX switches within the fabric.

.

Examples

This example specifies a non-Clos IP Fabric.

```
$ efa fabric setting --fabric-type non-clos
```

History

Release version	Command history
18s.1.01a	This command was introduced.

efa fabric show

Displays rack and device information for a non-Clos topology.

Syntax

efa fabric show

Modes

TPVM configuration mode

Examples

This example displays rack and device information for a non-Clos topology.

```
$ efa fabric show
+-------------------+-----------------+----------+-----------------------------------------+
|  IP ADDRESS       |  HOSTNAME       |  RACK    | MODEL     |               FIRMWARE                |
+-------------------+-----------------+----------+-----------------------------------------+
| 10.25.225.163   | 9140_03     | Rack-1   | 3001      | 18s.1.01_bld22                          |
| 10.25.225.167   | 9140_04     | Rack-1   | 3001      | 18s.1.01_bld22                          |
| 10.24.48.131    | 9140_05     | Rack-2   | 3001      | 18s.1.01_bld22                          |
| 10.24.51.135    | 9140_06     | Rack-2   | 3001      | 18s.1.01_bld22                          |
| 10.24.51.131    | 9140_07     | Rack-3   | 3001      | 18s.1.01slxos18s.1.01_pit_a_181001_1800 |
| 10.25.225.58    | 9140_08     | Rack-3   | 3001      | 18s.1.01slxos18s.1.01_pit_a_181001_1800 |
+-------------------+-----------------+----------+-----------+-----------------------------+
```

History

Release version	Command history
18s.1.01a	This command was introduced.

efa supportsave

Creates a supportSave .zip package that contains the EFA database and execution logs.

Syntax

efa supportsave

Command Default

supportSave is not configured by default.

Modes

TPVM configuration mode

Usage Guidelines

This command is executed in TPVM configuration mode on one of the SLX switches within the fabric.

The database and execution logs are available in `/var/efa/efa_SS.zip`.

Examples

This example creates a supportSave .zip package that contains the EFA database and execution logs on the switch.

```
$ efa supportsave
```

History

Release version	Command history
17s.1.02b	This command was introduced.

enable (PTP)

Enables or disables Precision Time Protocol (PTP) at the switch or interface level in global PTP configuration mode.

Syntax

enable

no enable

Modes

Global PTP configuration mode

Interface PTP configuration mode

Usage Guidelines

At the switch level:

- The default state is disabled. When it is enabled by the **enable** command in PTP configuration mode, the PTP feature is enabled on the switch. A PTP-aware switch functions as a boundary clock device, whereas a PTP-unaware switch functions as a Layer 2 switch.
- When PTP is disabled, the switch behaves as a PTP-unaware device, and PTP frames that are received are discarded.
- PTP can run on a fabric that consists of both PTP-aware and PTP-unaware switches. When a PTP-unaware switch is present, the end system in the communication path of these devices does not receive the level of clock accuracy supported by this feature.
- The **no** form of this command at the switch level disables existing PTP configurations and reverts to PTP-unaware mode.

At the interface level:

- The default state is disabled. When PTP is disabled at an interface but is enabled at the switch level, no PTP processing occurs on the port, and ingress PTP frames are discarded
- When PTP is enabled at both the switch and the interface level, PTP runs on the enabled interface.
- The **no** form of this command at the interface level causes PTP frames to be dropped.

Examples

To enter PTP configuration mode and enable PTP on the switch:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# enable
```

To disable PTP on the switch, leaving global PTP configurations unchanged:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# no enable
```

To enter PTP configuration mode and enable PTP on an 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)# enable
```

To disable PTP on an interface, leaving interface configurations unchanged:

```
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 enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

encoding (Telemetry)

Designates the encoding format for telemetry streaming.

Syntax

encoding { **gpb** | **json** }

Command Default

Encoding is set to Google protobuf (GPB).

Parameters

gpb

Designates GPB encoding for telemetry streaming.

json

Designates JavaScript Object Notation (JSON) encoding for telemetry streaming.

Modes

Telemetry collector configuration mode

Usage Guidelines

This command designates the encoding format for telemetry streaming.

Examples

Example of setting the encoding format to JSON.

```
device# configure terminal
Entering configuration mode terminal
device(config-collector_collector_1# ip 10.168.112.10 port 1
device(config-collector-collector_1)# encoding json
```

History

Release version	Command history
17s.1.03	This command was introduced.

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. A value of 7 specifies that 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 specifies 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 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 is set to 0.

Examples

The following example shows how to specify an encryption level of 0 so that 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

endpoint-tracking enable

Enables endpoint tracking on a Layer 2 (switchport) interface.

Syntax

endpoint-tracking enable

no endpoint-tracking enable

Command Default

Endpoint tracking is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

The interface must be configured as a Layer 2 (switchport) interface.

Use the **endpoint-tracking timeout reauth-period** command to configure the reauthentication timer.

Examples

The following example configures endpoint tracking configured on an interface configured as a switchport.

```
device# configure terminal
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)# endpoint-tracking enable
```

History

Release version	Command history
18s.1.01a, 18x.1.01	This command was introduced.

endpoint-tracking timeout reauth-period

Enables the endpoint-tracking timer and specifies the reauthentication timeout interval used by each session on the port.

Syntax

endpoint-tracking timeout reauth-period *seconds*

no endpoint-tracking timeout reauth-period

Command Default

The endpoint tracking reauthentication timer is disabled.

Parameters

seconds

Specifies an integer from 300 to 86400. The default is 300.

Modes

Interface subtype configuration mode

Usage Guidelines

The interface must be configured as a Layer 2 (switchport) interface.

If you enter this command when endpoint tracking is disabled, the timer is configured but endpoint tracking remains disabled. You must enter the **endpoint-tracking enable** command to enable endpoint tracking.

Examples

The following example configures endpoint tracking configured on an interface configured as a switchport, and configures the reauthentication timer.

```
device# configure terminal
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)# endpoint-tracking enable
device(conf-if-eth-0/1)# endpoint-tracking timeout reauth-period 1200
```

History

Release version	Command history
18s.1.01a, 18x.1.01	This command was introduced.

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

Modes

BGP configuration mode

Usage Guidelines

This command causes the device 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 **no** form of the command disables this feature.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

esi auto lacp

Configures the Ethernet Segment ID (ESI) auto generation based on the Partners LACP system MAC address and LACP port key. This ESI is ESI type 1 as defined in RFC 7432 Section 5.

Syntax

esi auto lacp

no esi auto lacp

Modes

Cluster client configuration mode

Usage Guidelines

Use the **no** form of the command to delete the ESI setting.

ESI is automatically generated.

LACP ESI is encoded as follows:

- 1 byte ESI type is 1
- 6 bytes Partners LACP system MAC address
- 2 bytes LACP port key
- Remaining byte is zero

ESI is generated when the partner LACP MAC and port key is learned.

Examples

The following example shows the setting of the ESI for the cluster client.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# esi auto lacp
```

History

Release version	Command history
17s.1.01	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

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.
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

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.

For additional usage guidelines regarding the advanced configuration commands, see the following topics:

- **action-timeout**
- **delay**
- **iterations**
- **interval**
- **trigger-mode**
- **trigger-function**

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**.

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
event-handler activate eventHandler1
device(config-activate-eventHandler1)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

evpn

Specifies an EVPN instance and enables EVPN instance configuration mode.

Syntax

evpn *instance*

no evpn *instance*

Command Default

This mode is disabled.

Modes

Global configuration mode

Parameters

instance

EVPN instance. Range is from 1 through 64 ASCII letters and numbers.

Usage Guidelines

Use the **no** form of this command to remove the EVPN instance.

Examples

The following example specifies an EVPN instance and enables EVPN instance configuration mode.

```
device# configure terminal
device(config)# evpn evpn1
device(config-evpn-evpn1)#
```

History

Release version	Command history
17s.1.01	This command was introduced.

evpn irb ve

Specifies an Ethernet VPN (EVPN) integrated routing and bridging (IRB) virtual Ethernet (VE) interface in a VRF for routing.

Syntax

evpn irb ve *VE*

no evpn irb ve *VE*

Command Default

This feature is not enabled.

Parameters

VE

VE interface number. Range is from 1 through 4096.

Modes

VRF configuration mode

Usage Guidelines

The IRB interface is the VE interface that is used for routing after tunnel termination. The IRB interface must belong to the tenant VRF and be administratively up. It is not necessary to configure an IP address on the IRB interface.

Use the **no** form of this command to delete the VE interface.

Examples

The following example specifies an EVPN IRB VE interface.

```
device# configure terminal
device(config)# vrf myvrf
device(config-vrf-myvrf)# evpn irb ve 10
```

History

Release version	Command history
17s.1.01	This command was introduced.

extend bridge-domain

Configures a switchport bridge domain (BD) or range of BDs for the tunnels to the containing site in VXLAN overlay gateway site configurations.

Syntax

extend bridge-domain { **add** | **remove** } *bd_id*

no extend bridge-domain

Parameters

add
Specifies a BD ID or range of BD IDs to be added to a tunnel.

remove
Specifies a BD ID or range of BD IDs to be removed from a tunnel.

bd_id
A BD ID or range of BD 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

Use the **no attach vlan** *vlan_id* command to remove all switchport configurations from the tunnels to the containing

The following example configures a switchport VLAN and range of VLANs.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-site-mysite)# extend bridge-domain add 10,20-30
```

History

Release version	Command history
17s.1.01	This command was introduced.

extend vlan

Configures switchport VLANs for the tunnels to the containing site in VXLAN overlay gateway site 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.

Examples

The following example configures a switchport VLAN and range of VLANs.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-site-mysite)# extend vlan add 10,20-30
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

The **no** form of the command disables BGP fast external fallover.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

fec mode

Configures settings for forward error correction (FEC) on an interface.

Syntax

fec mode { **auto** | **disabled** | **FC-FEC** | **RS-FEC** }

Command Default

FEC mode is **auto**.

Parameters

auto
Specifies autonegotiaion mode.

disabled
Disables FEC.

FC-FEC
Specifies FEC for Fibre Channel support.

RS-FEC
Specifies Reed-Solomon FEC.

Modes

Interface configuration mode

Usage Guidelines

FC-FEC mode can be applied only on 25G interfaces.

Links belonging to physical ports with different FEC configurations can form LAGs, or port-channels. However, in the case of a mismatch in the FEC status of the peer ports, the link will not come up.

When a port is administratively down, the current FEC status may not be displayed correctly.

Examples

The following example configures FC-FEC mode on a 25G interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# fec mode fc-fec
```

The following example disables FEC on the interface.

```
device(conf-if-eth-0/1)# fec mode disabled
```

History

Release version	Command history
17s.1.01	This command was introduced.
18s.1.01	The Usage Guidelines were modified.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.
```

History

Release version	Command history
17s.1.00	This command was introduced.

firmware download

Downloads the firmware on the local device.

Syntax

firmware download { **default-config** | **ftp** | **scp** | **sftp** | **tftp** | **usb** | **interactive** } [**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

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.

manual

Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This parameter is ignored when issued on a Top-of-Rack (ToR) device or in a chassis with only one management module.

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 node 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 both the active and standby MMs.

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

You can use one of the following options for firmware upgrade/downgrade; ISSU, coldboot, or default-config.

By default, if you enter the firmware download command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves an High Availability failover of the active management module and is non-disruptive. In contrast, both of the coldboot and default-config options involve system reboots and are disruptive to 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.

Examples

Example of firmware download without options (ISSU):

```
device# firmware download ftp directory /buildsjc/sre/SQA/slxos/17s.1.00/17s.1.00 host 10.31.2.27 user
releaseuser password releaseuser

Performing system sanity check...


This command will use the ISSU protocol to upgrade the system. It will cause a WARM 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 coldboot option:

```
device# firmware download ftp directory /buildsjc/sre/SQA/slxos/17s.1.00/17s.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/17s.1.00/17s.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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 **noactivatefirmware 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 both 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
Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This parameter is ignored when issued on a compact device or in a chassis with only one management module.

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.

You can use one of the following options for firmware upgrade/downgrade; ISSU, coldboot, or default-config.

By default, if you enter the firmware download command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves an High Availability failover of the active management module and is non-disruptive. In contrast, both of the coldboot and default-config options involve system reboots and are disruptive to 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.

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/17s.1.00/17s.1.00 host 10.31.2.27 user
releaseuser password releaseuser
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

You can use one of the following options for firmware upgrade/downgrade; ISSU, coldboot, or default-config.

By default, if you enter the firmware download command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves an High Availability failover of the active management module and is non-disruptive. In contrast, both of the coldboot and default-config options involve system reboots and are disruptive to 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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
Performs a firmware download 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.

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.

You can use one of the following options for firmware upgrade/downgrade; ISSU, coldboot, or default-config.

By default, if you enter the firmware download command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves an High Availability failover of the active management module and is non-disruptive. In contrast, both of the coldboot and default-config options involve system reboots and are disruptive to 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 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/slx17s.1.00/slx17s.1.00 host 10.31.2.27
user releaseuser password releaseuser
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
Performs a firmware download on the local switch.

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.

You can use one of the following options for firmware upgrade/downgrade; ISSU, coldboot, or default-config.

By default, if you enter the firmware download command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves an High Availability failover of the active management module and is non-disruptive. In contrast, both of the coldboot and default-config options involve system reboots and are disruptive to 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/slx17s.1.00/slx17s.1.00 host
10.31.2.27 user releaseuser password releaseuser
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
Performs a firmware download on the local device.

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.

You can use one of the following options for firmware upgrade/downgrade; ISSU, coldboot, or default-config.

By default, if you enter the firmware download command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves an High Availability failover of the active management module and is non-disruptive. In contrast, both of the coldboot and default-config options involve system reboots and are disruptive to 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/slx17s.1.00/slx17s.1.00 host 10.31.2.27
file release.plist
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 Technical Support.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

manual

Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This parameter is ignored when issued on a Top-of-Rack (ToR) device or in a chassis with only one management module.

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.

You can use one of the following options for firmware upgrade/downgrade; ISSU, coldboot, or default-config.

By default, if you enter the firmware download command without any options, the command invokes ISSU to upgrade the entire system. ISSU involves an High Availability failover of the active management module and is non-disruptive. In contrast, both of the coldboot and default-config options involve system reboots and are disruptive to 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_17s.1.00
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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

The following example restores 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 ...
```

History

Release version	Command history
17s.1.00	This command was introduced.

flow

In a UDA profile, specifies the expected packet structure.

Syntax

flow header0 *header0-type* [**header1** *header1-type* [**header2** *header2-type* [**header3** *header3-type* [**header4** *header4-type* [**header5** *header5-type* [**header6** *header6-type* [**header7** *header7-type*]]]]]]]

no flow header0 *header0-type* [**header1** *header1-type* [**header2** *header2-type* [**header3** *header3-type* [**header4** *header4-type* [**header5** *header5-type* [**header6** *header6-type* [**header7** *header7-type*]]]]]]]

Command Default

In a UDA profile, no expected packet-header types are defined.

Parameters

header0,1,2,3,4,5,6,7 *header0,1,2,3,4,5,6,7-type*

Specifies expected packet header-types. For supported values, refer to the Usage Guidelines.

Modes

UDA-profile configuration mode

Usage Guidelines

Ths command is supported only in NPB system mode.

You can specify up to eight headers types.

TABLE 3 Header types supported in UDA profiles

Value	Description
ETHERNET	Ethernet header
TUN_ETHERNET	Inner Ethernet header in tunneled frames
IPV4	IPv4 header
IPV6	IPv6 header
ARP	ARP header
TCP	TCP header
UDP	UDP header
SCTP	SCTP header
IGMP	IGMP header
ICMP	ICMP header
ICMPV6	ICMPv6 header
MPLS	MPLS header
GRE	GRE header

TABLE 3 Header types supported in UDA profiles (continued)

Value	Description
VXLAN	VXLAN header
GTP	GTP header
PAYLOAD4	Payload (4 bytes)
PAYLOAD8	Payload (8 bytes)
PAYLOAD16	Payload (16 bytes)
PAYLOAD32	Payload (32 bytes)

To delete a flow, use the **no** form of this command.

To modify a flow, delete the current flow and define a new one.

Examples

The following example configures a UDA profile, creates a flow, and specifies header types and fields.

```
device# configure terminal
device(config)# uda-key profile fkp1
device(conf-uda-profile-fkp1)# flow header0 ETHERNET header1 IPV4 header2 UDP header3 PAYLOAD32
device(conf-uda-profile-fkp1)# uda-key0 header0 ETHER_TYPE
device(conf-uda-profile-fkp1)# uda-key1 header1 PROTOCOL
device(conf-uda-profile-fkp1)# uda-key2 header2 DST_PORT
device(conf-uda-profile-fkp1)# uda-key3 header3 WORD1
```

History

Release version	Command history
18s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

Commands G - J

graceful-restart (BGP EVPN)

Enables the BGP graceful restart (GR) capability for BGP EVPN.

Syntax

graceful-restart

no graceful-restart

Command Default

This feature is disabled.

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

Use this command under BGP address-family L2VPN EVPN 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.

BGP EVPN GR helper is supported. However, BGP EVPN GR router restart is not supported.

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 **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 l2vpn evpn
device(config-bgp-evpn)# graceful-restart
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
```

History

Release version	Command history
18s.1.00	This command was introduced.

gtp-de-encapsulation

Enables the GPRS Tunneling Protocol (GTP) de-encapsulation feature on an interface.

Syntax

gtp-de-encapsulation

no gtp-de-encapsulation

Command Default

GTP de-encapsulation is not configured.

Modes

Physical interface configuration mode

Usage Guidelines

This feature is relevant only under NPB system mode, and supports only the GTPv1-U protocol.

This feature applies to both IPv4 and IPv6 traffic.

When GTP de-encapsulation is performed on a frame, only one C-tag is retained in the L2 header. Other tags—802.1BR, VN-Tag, S-Tag, and Outer C-Tag—are dropped from the L2 header.

If GTP de-encapsulation is applied to a frame, VLAN-header modification settings are ignored on that frame.

The final Frame Check Sequence (FCS) is updated with a recalculated CRC.

The **no** form of this command disables GTP de-encapsulation on the interface.

Examples

The following example enables the GTP de-encapsulation feature on an interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# gtp-de-encapsulation
```

The following example disables the GTP de-encapsulation feature on an interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no gtp-de-encapsulation
```

History

Release version	Command history
18s.1.00	This command was introduced.

hardware

Accesses hardware configuration mode to access the connector, port-group, and 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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Protocol LLDP configuration mode

Profile configuration mode

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

The following example sets the time interval to 10 seconds between the transmissions.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# hello 10
```

The following example sets the time interval to 8 seconds between the transmissions for a specific LLDP profile.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# profile test1
device(config-profile-test1)# hello 8
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example configures 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example sets 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

host

Configures a Host IPv4 and IPv6 management IP address and default gateway.

Syntax

host ipv4 [**address** *ipv4-address* | **gateway** *gateway-address*]

host ipv6 [**address** *ipv6-address* | **gateway** *gateway-address*]

Parameters

ipv4
Specifies Host IPv4 management IP or gateway.

ipv6
Specifies Host IPv6 management IP or gateway.

address *ipv4-address/ipv6-address/prefix*
Specifies IPv4 or IPv6 address for the Host management interface.

gateway *ipv4-address/ipv6-gateway-address*
Specifies IPv4 or IPv6 gateway for the Host management interface.

Modes

Privileged EXEC mode

Examples

The following example creates a Host IPv4 management IP address and default gateway.

```
device# host ipv4 address 192.168.1.111/1 gateway 192.168.1.1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 enabled.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

http server

Configures HTTP or HTTPS service on a device.

Syntax

http server use-vrf *vrf-name* [**secure-and-plain**] [**shutdown**]

http server shutdown

no http server use-vrf *vrf-name* [**secure-and-plain**] [**shutdown**]

no http server shutdown

Parameters

use-vrf *vrf-name*
Specifies a user-defined VRF.

secure-and-plain
Allows the enabling or disabling of both HTTP and HTTPS simultaneously. The HTTPS certificate must be installed for this option to function correctly.

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 **secure-and-plain** parameters to enable both HTTP and HTTPS service for the specified VRF. The **secure-and-plain** parameter allows you to enable HTTP and HTTPS simultaneously. Without this option, you may only enable HTTP or HTTPS, but not both.

Use the **http server** command with the **use-vrf** and **shutdown** parameters to disable HTTP or HTTPS service for the specified VRF. When both HTTP and HTTPS are enabled, executing the **http server** command with the **use-vrf** and **shutdown** parameters disables both HTTP and HTTPS at the same time.

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.

Use the **no http server** command with the **use-vrf** and **secure-and-plain** parameters to disable HTTP and run HTTPS alone. This form of the command removes the **secure-and-plain** option from the running configuration.

Use the **http server** command with the **shutdown** parameter to disable HTTP or HTTPS service on the management VRF. Use the **no http server** command with the **shutdown** parameter to re-enable HTTP or HTTPS service on management VRF.

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 creates and enables both HTTP and HTTPS service on a device for a user-defined VRF.

```
device# configure terminal
device(config)# http server use-vrf myvrf secure-and-plain
```

When both HTTP and HTTPS service are enabled, the following command disables HTTP and runs HTTPS alone.

```
device# configure terminal
device(config)# no http server use-vrf myvrf secure-and-plain
```

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
```

The following example disables HTTP or HTTPS service on a device for the management VRF.

```
device# configure terminal
device(config)# http server shutdown
```

The following example enables HTTP or HTTPS service on a device for the management VRF.

```
device# configure terminal
device(config)# no http server shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

insight enable

Configures a port-channel as an insight interface.

Syntax

insight enable

no insight enable

Command Default

The insight interface is down until it is added to a port-channel by means of this command.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of this command to disable an insight interface on the port-channel.

Examples

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
```

Use the **show interface port-channel** and show port-channel commands to confirm the configuration.

```
device# show interface port-channel 33
Port-channel 33 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 0/12   *
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example maps 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

interface (telemetry)

Specifies monitored interfaces for telemetry profile-types.

Syntax

interface { **ethernet** | **port-channel** } **all**

interface { **ethernet** | **port-channel** } **add** *interfaces*

interface { **ethernet** | **port-channel** } **except** *interfaces*

interface { **ethernet** | **port-channel** } **remove** *interfaces*

interface { **ethernet** | **port-channel** } **none**

Command Default

No interfaces are defined and the profile is inactive.

Parameters

ethernet
Specifies ethernet interfaces.

port-channel
(Supported only for the **interface** and **pbr** profile types) Specifies port-channel interfaces.

all
Monitors all device interfaces.

add
Adds interfaces for monitoring.

except
Monitors all interfaces except for the ones specified.

remove
Removes the specified interfaces from monitoring.

none
Monitors no interfaces.

interfaces (ethernet)
Specifies physical interfaces, up to 1000 characters. The supported 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`

interfaces (port-channel)
(Supported only for the **interface** and **pbr** profile types) Specifies port-channel interfaces. The supported options are:

- *number*, for example, `10`
- *number***-***number*, for example, `5-8`

Modes

Telemetry profile configuration mode

Usage Guidelines

(For the **enhanced-queue-discard-pkts**, **interface**, **lldp**, **pbr**, and **queue** profile types) Without this parameter configured, the profile has no effect. Other profile types do not support the **interface** command.

To specify a combination of interfaces and interface ranges, separate them with commas.

To specify both ethernet and port-channel interfaces, use both an **interface ethernet** and an **interface port-channel** command.

Examples

The following example adds a range of ports and a port for monitoring.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# interface ethernet add 0/3-5,0/7
```

The following example adds all port-channels for monitoring.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# interface port-channel all
```

The following example removes a port from monitoring.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# interface ethernet remove 0/7
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.02	This command was modified, adding keywords and support for more profiles.

interface ethernet

Configures an Ethernet interface

Syntax

interface ethernet { *slot/port* }

Command Default

No Ethernet interface is configured.

Parameters

slot/port

Specifies a slot and port. Slot must be **0** for devices that do not contain line cards.

Modes

Global configuration mode

Examples

To configure interface Ethernet 0/1 on a device that does not contain line cards:

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

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

interface management

Accesses management interface configuration mode for the specified management interface.

Syntax

interface management 0

Parameters

0

Accesses the configuration mode for management interface 0.

Modes

Global configuration mode

Usage Guidelines

The mode allows you to configure the parameters of the specified management interface.

Examples

The following example accesses the interface management mode for management interface 0.

```
device# configure terminal
device(config)# interface Management 0
device(config-Management-0)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

interface port-channel

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. Range is from 1 through 1024.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable the interface.

Examples

To configure a port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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.

Use the **no** form of this command to remove a specified VE interface.

Examples

The following example shows the steps needed to create 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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** and the **pbr** profile-types, the default value is 60 seconds.

For the queue profile-types, the default value is 300 seconds.

Parameters

seconds

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 **pbr** profile-type and 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

Typical command execution.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# interval 255
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.00	Support was added for **enhanced-queue-discard-pkts** and **queue** profile types.
18s.1.02	Support was added for **lldp** and **pbr** profile types

ip access-group (general)

Applies rules specified in an IPv4 access control list (ACL) to traffic entering or exiting an interface.

Syntax

ip access-group *ACLname* { **in** | **out** } [**switched** | **routed**]

no ip access-group *ACLname* { **in** | **out** } [**switched** | **routed**]

Parameters

ACLname
Specifies the name of the standard or extended IPv4 ACL.

in
Applies the ACL to incoming switched and routed traffic.

out
Applies the ACL to outgoing routed traffic.

switched
Filters only switched traffic. This parameter is not valid for the management interface.

routed
Filters only routed traffic. This parameter is not valid for the management 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
  - (Ingress only) Physical Ethernet interfaces
  - (Ingress only) Logical interfaces (LAGs)
  - Virtual Ethernet interfaces (VEs)
- The management interface

You can apply a maximum of six ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- (VLANs only) One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- (VEs only) One egress IPv4 ACL
- One ingress IPv6 ACL
- (VEs only) One egress 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.

Examples

The following example applies an ingress IP ACL on an Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# ip access-group ipacl2 in
```

The following example removes an ingress IP ACL from an Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# no ip access-group ipacl2 in
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip access-group (overlay)

Applies rules specified in an IPv4 ACL to traffic entering or traversing a tunnel.

Syntax

ip access-group *ACLname*

no ip access-group *ACLname*

Parameters

ACLname

Specifies the name of the standard or extended IPv4 ACL.

Modes

Overlay transit configuration mode

Overlay gateway configuration mode

Usage Guidelines

This command is supported in overlay-policy maps applied both for overlay transit and for overlay gateway.

You can apply an ACL to multiple overlay-policy-map stanzas.

To remove an ACL from a stanza, enter the **no** form of this command.

Examples

The following example configures an IP ACL and an overlay class map. Then the policy map is created and a stanza (#10) is added. This stanza uses the class map "tunnel-group-1" to identify the gateway and specifies the IP ACL "test" on the flows within the tunnel. Finally there is a creation of the overlay gateway "gw2" and the overlay policy is applied, using the **overlay-service-policy in** command . The policy map can also applied to the overlay-transit (using the same command).

```
device# configure terminal
device(config)# ip access-list extended test
device(conf-ipacl-ext)# seq 10 deny ip host 192.85.1.2 host 192.0.0.1 count
device(conf-ipacl-ext)# seq 20 deny ip host 174.174.174.174 host 171.171.171.171 count
device(conf-ipacl-ext)# seq 30 deny ip host 171.1.0.0 host 174.1.0.0 count
device(conf-ipacl-ext)# exit

device(config)# overlay-class-map tunnel-group-1
device(config-overlay-classmap-tunnel-group-1)# seq 10 match source 1.1.1.1 destination 3.3.3.3
device(config-overlay-classmap-tunnel-group-1)# exit

device(config)# overlay-policy-map fooMap
(config-overlay-policymap-fooMap)# seq 10 overlay-class tunnel-group-1
device(config-overlay-policymap-class-tunnel-group-1) #ip access-group test
device(config-overlay-policymap-class-tunnel-group-1)# exit
device(config-overlay-policymap-fooMap)# exit

device(config)# overlay-gateway gw2
device(config-overlay-gw-gw2)# type layer2-extension
device(config-overlay-gw-gw2)# ip interface Loopback 1
device(config-overlay-gw-gw2)# map vni auto
device(config-overlay-gw-gw2)# overlay-service-policy in fooMap
device(config-overlay-gw-gw2)# site site_2
device(config-site-site_2)# ip address 1.1.1.1
device(config-site-site_2)# extend vlan add 50,60,70
device(config-site-site_2)# activate
device(config-overlay-gw-gw2)# exit
```

History

Release version	Command history
17s.1.00	This command was introduced, for security ACLs.
17s.1.01	This Overlay Services version of this command was introduced.

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** form of this command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using a **no access-group** command.

Examples

The following example creates an IPv4 standard ACL.

```
device# configure terminal
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(conf-ipacl-std)# seq 5 permit host 10.20.33.4
device(conf-ipacl-std)# seq 15 deny any
```

The following example deletes an IPv4 ACL.

```
device# configure terminal
device(config)# no ip access-list standard stdACL3
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip address

Configures an IP address on an interface.

Syntax

ip address *ip-address/mask* [**secondary**] [**ospf-ignore**] [**ospf-active**]

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 configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary 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

Usage Guidelines

- Use this command to configure a primary or secondary IP address for a specific 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 a management interface.
- For a management interface, only one primary IP address is supported. Secondary IP addresses are not supported.
- A primary IP address cannot overlap with a previously 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**.
- The **no** form of the command removes a specific IP address from the interface.

Examples

The following example configures a primary IP address on a specified Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ip address 10.1.1.1/24
```

The following example configures a secondary IP address on a specified Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ip address 10.1.1.2/24 secondary
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip address (VXLAN)

Specifies the destination IPv4 address of a tunnel in VXLAN overlay gateway site configurations.

Syntax

ip address *IPv4_address*

no ip address [*IPv4_address*]

Parameters

IPv4_address
IPv4 address of the destination tunnel.

Modes

VXLAN overlay gateway 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

To specify an IPv4 address of a destination tunnel:

```
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
```

History

Release version	Command history
17s.1.01	This command was introduced.

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

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 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
!
```

History

Release version	Command history
17s.1.01	This command was introduced.

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 0/4
device(conf-if-eth-0/4)# ip arp-aging-timeout 100
```

The following command restores the ARP aging timeout to the default value of 25 minutes on an interface.

```
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# no ip arp-aging-timeout
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified to reflect the default timeout change from 240 to 25 minutes.

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 applies ARP_ACL_01 to VLAN 200 and enables DAI.

```
device# configure terminal
device(conf)# vlan 200
device(conf-vlan-200)# ip arp inspection filter ARP_ACL_01
device(conf-vlan-200)# ip arp inspection
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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 removes the current ARP ACL from the VLAN.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Usage Guidelines

This command is effective only on a Layer 3 interface.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip as-path access-list

Configures an AS-path access control list (ACL), specifies the community name, and whether to permit or deny traffic.

Syntax

ip as-path access-list *string* { **deny** *regular-expression* | **permit** *regular-expression* } [**seq** *seq-value*]

no ip as-path access-list *string* { **deny** *regular-expression* | **permit** *regular-expression* } [**seq** *seq-value*]

Parameters

string
Specifies an ACL name, from 1 to 32 ASCII characters in length.

deny *regular-expression*
Denies a matching pattern based on a regular expression, a string inside quotes.

permit *regular-expression*
Permits a matching pattern based on a regular expression, a string inside quotes.

seq *seq-value*
Specifies a sequence value. Valid values range from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

Regular expressions must be enclosed in quotes.

Examples

The following example creates an AS-path ACL that permits a matching pattern and specifies a regular expression.

```
device# configure terminal
device(config)# ip as-path access-list seq 10 permit "myaspath"
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip community-list extended

Configures a community access control list (ACL), specifies the community name, and whether to permit or deny traffic, including through the use of a regular expression.

Syntax

ip community-list extended *community-list-name* { **deny** *string* | **permit** *string* } [**seq** *seq*]

no ip community-list extended *community-list-name*

Parameters

community-list-name
Specifies an ACL, from 1 through 32 ASCII characters in length.

deny *regular-expression*
Denies a matching pattern based on a regular expression, a string inside quotes.

permit *regular-expression*
Permits a matching pattern based on a regular expression, a string inside quotes.

seq *seq-value*
Specifies a sequence value. Valid values range from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

Unlike a standard community list, this command does accept a regular expression as long as the string is enclosed in quotes.

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 community-list extended seq 10 permit "mycommunity"
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip community-list standard

Configures a community access control list (ACL), specifies the community number or type, and whether to permit or deny traffic.

Syntax

ip community-list standard *community-list-name* { **deny** [*community-number* | *AA:NN*] | **permit** *community-number* } [**seq** *seq-value*] [**internet** | **local-as** | **no-advertise** | **no-export**]

ip community-list standard *community-list-name* { **deny** | **permit** } { *community-number* | *AA:NN* | **internet** | **local-as** | **no-advertise** | **no-export** }

ip community-list standard *community-list-name* **seq** *seq-value* { **deny** | **permit** } { *community-number* | *AA:NN* | **internet** | **local-as** | **no-advertise** | **no-export** }

no ip community-list standard *community-list-name*

Parameters

community-list-name
: Range is from 1 through 32 ASCII characters.

deny
: Denies a matching pattern based on a regular expression.

permit
: Permits a matching pattern based on a regular expression.

community-number
: Specifies a community number. Range is from 1 through 4294967295.

AA **:** *NN*
: Specifies an autonomous system number and network number, configured as 2-byte numbers separated by a colon.

internet
: Specifies the Internet community.

no-export
: Specifies a community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs in the same confederation but not outside the confederation to other ASs or otherwise sent to EBGP neighbors.

local-as
: Specifies a local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.

no-advertise
: Specifies that routes with this community cannot be advertised to any other BGP4 devices at all.

seq *seq-value*
: Speccifies a sequence value. Valid values range from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

A standard community list does not accept a regular expression.

There are two ways to delete a filter from the list. The first is by sequence number parameter **no ip community-list standard** *community-list-name* **seq** *seq-value*. The second is executing the syntax **no ip community-list standard** *community-list-name* , resulting in all filters within the community list, as well as the community list container, being removed from the configuration database.

Examples

The following example creates a standard community list.

```
device# configure terminal
device(config)# ip community-list standard seq 10 permit local-as
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example configures an IP DHCP Relay address on a Ve interface.

```
device# configure terminal
device(config)# interface ve 100
device(config-Ve-100)# ip dhcp relay address 3.1.2.255 use-vrf blue
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip dhcp relay gateway address

Configures the IP DHCP Relay on a Layer 3 gateway interface.

Syntax

ip dhcp relay gateway address *ip-addr*

no ip dhcp relay gateway address *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# configure terminal
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# ip dhcp relay gateway 10.50.22.26
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip dhcp relay information option

Enables DHCP Relay Agent Information Option 82 on a VLAN.

Syntax

ip dhcp relay information option

no ip dhcp relay information option

Command Default

DHCP Relay Agent Information Option 82 is not enabled.

Modes

VLAN configuration mode

Usage Guidelines

Use the **no** form of this command to disable DHCP Relay Agent Information Option 82.

Examples

The following example enables DHCP Relay Agent Information Option 82 on a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ip dhcp relay information option
```

The following example disables DHCP Relay Agent Information Option 82 on a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# no ip dhcp relay information option
```

History

Release version	Command history
17s.1.01	This command was introduced.
	This command was modified to...

ip dns

Configures the Domain Name System (DNS) domain name and the primary and secondary name server IP addresses.

Syntax

ip dns { **domain-name** *domain-name* | **name-server** *ip-address-of-name-server* }

no ip dns { **domain-name** *domain-name* | **name-server** *ip_address_of_name_server* }

Parameters

domain-name *domain-name*
Specifies the DNS domain name.

name-server *ip-address-of-name-server*
Specifies the IP address of the name server. IPv6 and IPv4 addresses are supported.

Modes

Global configuration mode

Usage Guidelines

- Your first run of **ip dns name-server** specifies the default IP gateway address. Your second run of **ip 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.
- The **no** form of the command with the domain-name parameter disables IP directed broadcasts for a specific domain.
- The **no** form of the command with the name-server parameter deletes a name server definition.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

This command is enabled on the management port, but is disabled on the front-end ports.

Parameters

milliseconds

Time interval per ICMP packet in milliseconds. The range is from 0 through 4294967295. The default is 1000.

Modes

Interface 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# configure terminal
device(config)# interface ethernet 0/1
device(conf-int-eth-0/1)# ip icmp rate-limiting 10000
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

This command is enabled on both the management port and on the front-end ports.

Modes

Interface configuration mode

Usage Guidelines

This is an interface-specific configuration.

The **no** form of the command disables IPv4 ICMP Redirect messages.

Examples

The following example enables IPv4 ICMP Redirect messages on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-int-eth-0/1)# ip icmp redirect
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip igmp snooping enable

Enables Internet Group Management Protocol (IGMP) snooping.

Syntax

ip igmp snooping enable

no ip igmp snooping enable

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# configure terminal
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

This command is disabled.

Modes

VLAN configuration mode.

Usage Guidelines

Enter **no ip igmp snooping fast-leave** 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip igmp snooping last-member-query-count

Sets the last member query count for a routed port. The last member query count is used while processing the leave message.

Syntax

ip igmp snooping last-member-query-count *value*

no ip igmp snooping last-member-query-count *value*

Command Default

The default value is 2.

Parameters

value

Range is from 2 through 10. The default is 2.

Modes

VLAN configuration mode

Usage Guidelines

The IGMP snooping query maximum response time is the length of time in seconds that the device will wait for 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 last member query count.

```
device# configure terminal
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping last-member-query-count 3
```

History

Release version	Command history
17s.1.00	This command was introduced.

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# configure terminal
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping last-member-query-interval 2000
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* }

Parameters

ethernet*slot/port*
Specifies a valid port number.

port-channel *number*
Specifies the interface is a port-channel. Valid values range from 1 through 6144.

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# configure terminal
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping mrouter interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip igmp snooping querier enable

Activates or deactivates 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

IGMP snooping querier is disabled.

Modes

VLAN configuration mode

Usage Guidelines

Enter **no ip igmp snooping querier enable** to disable the IGMP snooping querier.

Examples

The following example enables the IGMP snooping querier on the VLAN.

```
device# configure terminal
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping querier enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 default is 125 seconds.

Parameters

seconds

Sets the IGMP snooping query interval in seconds. The range is from 1 through 18000 seconds.

Modes

VLAN configuration mode

Usage Guidelines

The **ip igmp snooping query-interval** command allows you to modify the query interval, which specifies how often a device enabled for active IGMP snooping sends group membership queries.

Examples

The following example sets the IGMP snooping query interval.

```
device# configure terminal
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping query-interval 200
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 default is 10 seconds.

Parameters

seconds

Specifies the IGMP snooping query maximum response time in seconds. The range is 1 to 25 seconds.

Modes

VLAN configuration mode

Usage Guidelines

The IGMP snooping query maximum response time is the length of time in seconds that the device will wait for 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# configure terminal
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping query-max-response-time 15
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip igmp snooping restrict-unknown-multicast

Stops the flooding of unknown multicast traffic in a VLAN domain.

Syntax

ip igmp snooping restrict-unknown-multicast

no igmp snooping restrict-unknown-multicast

Command Default

IGMP snooping restrict-unknown-multicast is enabled.

Modes

VLAN configuration mode

Usage Guidelines

The hardware profile ipv4-v6-mcast must be enabled, by means of the hardware-profile command.

Using the **no ip igmp snooping restrict-unknown-multicast** command will flood multicast traffic to all members of the VLAN.

Examples

To stop the flooding of unknown multicast traffic for a VLAN enter the following commands:

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# ip igmp snooping restrict-unknown-multicast
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip igmp snooping robustness-variable

Configures a value to compensate for IGMP snooping packet loss in congested networks.

Syntax

ip igmp snooping robustness-variable *value*

no ip igmp snooping robustness-variable *value*

Command Default

See parameters.

Parameters

value

The number of general IGMP snooping queries sent before a multicast address is aged out. The range is from 2 through 10. The default is 2.

Modes

VLAN configuration mode

Usage Guidelines

This value determines the number of general IGMP snooping queries that are sent before a multicast address is aged out for lack of a response. Use this command to configure the robustness variable. This command is supported on port-channel, and VLAN interfaces.

The **no** form of the command restores the robustness variable value to 2 (the default).

Examples

The following example changes the robustness variable on a VLAN to 7.

```
device# configure terminal
device(config)# vlan 2000
device(config-vlan-2000)# ip igmp snooping robustness-variable 7
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip igmp snooping startup-query-count

Sets the IGMP startup query count for an interface.

Syntax

ip igmp snooping startup-query-count *value*

no ip igmp snooping startup-query-count *value*

Command Default

See Parameters.

Parameters

value

The number of queries sent at startup. The range is from 1 through 10. The default is 2.

Modes

VLAN configuration mode

Usage Guidelines

This command is useful when the IGMP querier starts the first time. This command is supported on port-channel and VLAN interfaces.

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

Examples

The following example changes the IGMP startup query count on a VLAN from the default to 3.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# ip igmp startup-query-count 3
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip igmp snooping startup-query-interval

Sets the IGMP startup query interval for an interface.

Syntax

ip igmp snooping startup-query-interval *seconds*

no ip igmp snooping startup-query-interval *seconds*

Command Default

See Parameters.

Parameters

seconds

The response time in seconds. Range is from 1 through 450. The default is 31.

Modes

VLAN configuration mode

Usage Guidelines

This command is useful when the IGMP querier starts the first time. This command is supported on port-channel and VLAN interfaces.

The **no** form of the command restores the startup query interval to the default.

Examples

The following example sets the IGMP startup query interval for a VLAN to 200 seconds.

```
device# configure terminal
device(config)# vlan 100
device(conf-vlan-100)# ip igmp startup-query-interval 20
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* }

ip igmp snooping static-group { *ip-address* } {**interface** *ethernet/port-channel* }

Parameters

ip-address

Specifies the multicast address to be joined in the 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 sets the IGMP snooping static-group.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ip igmp snooping static-group 225.0.0.1 interface ethernet 0/4
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip interface

Configures a loopback or a virtual Ethernet (VE) interface as a Layer 3 interface for a VXLAN overlay gateway.

Syntax

ip interface { **loopback** *loopback_id*| **ve** *ve_id* **vrrp-extended-group** *vrrp_id*}

no ip interface { **loopback** *loopback_id*| **ve** *ve_id* **vrrp-extended-group** *vr_id*}

Command Default

This feature is not enabled.

Parameters

loopback*loopback_id*

Specifies a loopback interface. Range is from 1 through 255.

ve*ve_id*

Specifies a VE interface. Range is from 1 through 4096.

vrrp-extended-group*vr_id*

Specifies a virftual router identifier (VRID) for VRRP-E. Range is from 1 through 255.

Modes

VXLAN overlay gateway configuration mode.

Usage Guidelines

Use the **no** form of this command to delete a Layer 3 interface.

Examples

The following example configures a loopback interface as a Layer 3 interface.

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# ip interface loopback 10
```

The following example configures a VE interface as a Layer 3 interface and specifies a VRRP-E router ID.

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# ip interface ve 10 vrrp-extended-group 10
```

The following example deletes a Layer 3 loopback interface.

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# no ip interface loopback 10
```

History

Release version	Command history
17s.1.01	This command was introduced.

ip mtu

Sets the IP Maximum Transmission Unit (MTU) on an interface or globally.

Syntax

ip mtu *size*

no ip mtu

Command Default

The default IP MTU size is 1500 bytes.

Parameters

size

Specifies the size of an interface IP MTU. Values range from 1300 through 9194 bytes.

Modes

Global configuration mode

Interface configuration mode

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.

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.

The **no** form of the command reverts the MTU size to the default value.

Examples

The following example sets the IP MTU to 2000 bytes globally.

```
device# configure terminal
device(config)# ip mtu 2000
```

The following example sets the IP MTU to 2000 bytes on the specified Ethernet interface.

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

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified to include support for global configuration mode.

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 0/1
device(conf-if-eth-0/1)# ip ospf active
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip ospf area

Enables OSPFv2 on an interface.

Syntax

ip ospf area *area-id* | *ip-addr*

no ip ospf area

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Parameters

wait-time

Time before an authentication change takes place. Valid values range from 0 to 14400 seconds. The default is 300 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/4
device(conf-if-eth-0/4)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip ospf cost

Configures cost for a specific interface.

Syntax

ip ospf cost *value*

no ip ospf cost

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# ip ospf database-filter all-out
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535. The default is 10 seconds.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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.

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 0/1
device(conf-if-eth-0/1)# 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 0/1
device(conf-if-eth-0/1)# ip ospf md5-authentication key-id 22 key myospfpassword
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

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 0/1
device(conf-if-eth-0/1)# 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 0/1
device(conf-if-eth-0/1)# ip ospf mtu-ignore
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# 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 0/1
device(conf-if-eth-0/1)# ip ospf network broadcast
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# ip ospf passive
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip ospf priority

Configures priority for designated router (DR) election.

Syntax

ip ospf priority *value*

no ip ospf priority

Parameters

value

Priority value. Valid values range from 0 through 255. The default is 1.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Parameters

interval

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds. The default is 5 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 0/1
device(conf-if-eth-0/1)# ip ospf retransmit-interval 8
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds. The default is 1 second.

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 0/1
device(conf-if-eth-0/1)# ip ospf transmit-delay 25
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip policy route-map

Enables the IP route map.

Syntax

ip policy route-map *map-name*

no ip policy route-map *map-name*

Command Default

The IP route map is not enabled.

Parameters

map-name

Specifies the name of the IP route map.

Modes

Route map configuration mode

Interface configuration mode

Virtual interface configuration mode

Usage Guidelines

The **no** form of the command disables the IP route map.

Examples

The following example enables the IP route map 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 0/1
device(conf-if-eth-0/1)# ip policy route-map test-route
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip port (telemetry)

Specifies the IPv4 or IPv6 address and port of a telemetry collector.

Syntax

ip *ip-address* **port** *port-number*

no ip

ipv6 *ipv6-address* **port** *port-number*

no ipv6

Command Default

No IPv4 or IPv6 address is designated.

Parameters

ip-address
Specifies the IPv4 address of a telemetry collector.

port *port-number*
Specifies a valid port number.

ipv6-address
Specifies the IPv6 address of a telemetry collector.

Modes

Telemetry-collector configuration mode

Usage Guidelines

To remove the IPv4 or IPv6 configuration from the collector, use the relevant **no** command.

Examples

The following example specifies an IPv4 address and port for the telemetry collector.

```
device# configure terminal
device(config)# telemetry collector collector_1
device(config-collector-collector_1)# ip 192.0.2.61 port 1
```

The following example specifies an IPv6 address and port for the telemetry collector.

```
device# configure terminal
device(config)# telemetry collector collector_2
device(config-collector-collector_2)# ipv6 11::11 port 1111
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.02	This command was modifed for IPv6 support.

ip prefix-list

Command for adding and deleting a filter from a standard community.

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

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.

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 packet that contains 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.

permit *ip-prefix/prefix-length*
Permits a packet that contains 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*
If you specify only **ge** *ge-value*, then the range is from *ge-value* to 32.

*le-value***le** *le-value*
If you specify only **le** *le-value*, then the range is from *le-value* to the *prefix-length* parameter.

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.

You are allowed to insert and delete rules anywhere in the ACL, but updates are not allowed. You can delete and add a new rule at the same location to simulate an update of an already existing rule.

A list rule added without a sequence number is allocated a sequence number. The allocated sequence number will be N greater than the largest sequence number of all the rules in the list where N is the increment value of 5. The rule add operation will fail if the allocated sequence number is not in the allowed sequence number range.

You are not allowed to delete a prefix list if it is actively being used by a client (such as a routing protocol).

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.

```
device# configure terminal
device(config)# ip prefix-list test deny 10.0.0.0/8 ge 20 le 28
device(config)# ip prefix-list test permit 10.1.0.0/16
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/4
device(conf-if-eth-0/4)# ip proxy-arp
```

The following example disables Proxy ARP on a specified interface.

```
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# no ip proxy-arp
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified, with Proxy ARP now disabled by default.

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* **in**

no ip receive access-group *acl-name* **in**

Command Default

No receive-path ACLs are applied.

Parameters

acl-name
: Specifies the name of the standard or extended IP access list.

in
: Specifies ingress traffic.

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 two receive-path ACLs to a device, as follows:

- One IPv4 receive-path ACL
- One IPv6 receive-path ACL

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 in
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*]

ip route *dest-ip-addr* { **ethernet** *slot/port* | **ve** *ve-number*} [*metric*] [**distance** *distance*] [**tag** *tag-number*]

ip route *dest-ip-addr* **null 0** [*metric*] [**distance** *distance*] [**tag** *tag-number*]

no ip route *dest-ip-addr* [**next-hop-vrf** *next-vrf-name*] *next-hop-address* [*metric*] [**distance** *distance*] [**tag** *tag-number*]

no ip route *dest-ip-addr* { **ethernet** *slot/port* | **ve** *ve-number* } [*metric*] [**distance** *distance*] [**tag** *tag-number*]

no ip route *dest-ip-addr* **null 0** [*metric*] [**distance** *distance*] [**tag** *tag-number*]

Parameters

next-hop-vrf *vrf-name*
Specifies the name of the non-default VRF to be used 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. Slot number must be 0 if the device does not contain slots.

next-hop-vrf *next-vrf-name*
VRF name of next hop.

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, supported devices prefer 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.

Modes

Global configuration mode or VRF IPv4 address-family 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 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 a supported-device interface.

> NOTE
> When you configure an interface as the next hop, an extra ARP entry is created for the destination IP address.

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 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# configure terminal
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# configure terminal
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.

```
device# configure terminal
device(config)# ip route 192.128.2.0/24 ethernet 0/1
```

The following example configures a null static route to drop packets destined for network 10.157.22.x.

```
device# configure terminal
device(config)# ip route 10.157.22.0/24 null 0
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip route static bfd

Configures Bidirectional Forwarding Detection (BFD) session parameters for IP static routes.

Syntax

ip route static bfd *dest-ip-address source-ip-address* [**interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

no ip route static bfd *dest-ip-address source-ip-address*

Command Default

BFD is not configured for an IP static route.

Parameters

dest-ip-address
Specifies the destination IP address.

source-ip-address
Specifies the source IP 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 500.

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 500.

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

Address-family IPv4 unicast VRF configuration mode

Global configuration mode

Usage Guidelines

The **interval** *transmit-time* and **min-rx** *receive-time* parameters are the intervals desired by the local device. The actual values in use will be the negotiated values.

For single-hop static BFD sessions, timeout values are optional because all required information is available from the outgoing interface. For multihop BFD sessions, if the configured **interval** and **min-rx** parameters conflict with those of an existing session, the lower values are used.

If you configure a neighbor IP address and a source IP address that already exist in BFD, BFD overwrites the existing interval values and multiplier for the IP addresses with the new values, on behalf of the static module.

Static BFD can be configured without configuring a static route to configure a BFD session. This is especially useful on BFD neighbors when they have reachability from other neighbors via OSPF or BGP. You must configure different BFD sessions for each ECMP path with the corresponding interface IP as the source IP address.

The **no** form of the command removes the configured BFD IP static route.

Examples

The following example configures a BFD session on an IP 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
```

The following example configures a BFD session on an IP static route in a nondefault VRF instance.

```
device# configure terminal
device(config)# vrf orange
device(config-vrf-orange)# address-family ipv4 unicast
device(vrf-orange-ipv4-unicast)# ip route static bfd 10.2.2.2 10.3.3.3 interval 600 min-rx 700
multiplier 10
```

History

Release version	Command history
17s.1.00	This command was introduced.

ip route static bfd holdover-interval

Sets the time interval for which Bidirectional Forwarding Detection (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 *time*

Parameters

time

Specifies BFD holdover interval in seconds. Valid values range from 1 through 30. The default is 0.

Modes

Address-family IPv4 unicast VRF configuration mode

Global configuration mode

Usage Guidelines

If the BFD session is restored within the specified time interval, no down notification is sent.

Use the **ip route static bfd holdover-interval** command in global configuration mode to set the BFD holdover interval globally for static routes.

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 for IP static routes to 15.

```
device# configure terminal
device(config)# ip route static bfd holdover-interval 15
```

The following example removes the configured BFD holdover interval for IP static routes.

```
device# configure terminal
device(config)# no ip route static bfd holdover-interval
```

The following example sets the BFD holdover interval in a nondefault VRF instance.

```
device# configure terminal
device(config)# vrf orange
device(config-vrf-orange)# address-family ipv4 unicast
device(vrf-orange-ipv4-unicast)# ip route static bfd holdover-interval 15
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 virtual Ethernet (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 Virtual Ethernet interface 20.

```
device# configure terminal
device(config)# protocol vrrp-extended
device(config)# interface ve 20
device(config-if-Ve-20)# ip vrrp-extended auth-type md5-auth lyk28d3j
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 access-group (general)

Applies rules specified in an IPv6 access control list (ACL) to traffic entering or exiting an interface.

Syntax

ipv6 access-group *ACLname* { **in** | **out** } [**switched** | **routed**]

no ipv6 access-group *ACLname* { **in** | **out** } [**switched** | **routed**]

Parameters

ACLname
Specifies the name of the standard or extended IPv6 access list.

in
Applies the ACL to incoming switched and routed traffic.

out
Applies the ACL to outgoing routed traffic.

switched
Filter only switched traffic. This parameter is not valid for the management interface.

routed
Filter only routed traffic. This parameter is not valid for the management interface.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to apply an IPv6 ACL to one of the following interface types:

- User interfaces
  - (Ingress only) Physical Ethernet interfaces
  - (Ingress only) Logical interfaces (LAGs)
  - Virtual Ethernet interfaces (VEs)
- The management interface

You can apply a maximum of six ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- (VLANs only) One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- (VEs only) One egress IPv4 ACL
- One ingress IPv6 ACL
- (VEs only) One egress 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.

Examples

The following example applies an IPv6 ACL on an Ethernet interface to incoming traffic.

```
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(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no ipv6 access-group ipv6_acl_7 in
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 access-group (overlay)

Applies rules specified in an IPv6 ACL to traffic entering or traversing a tunnel.

Syntax

ipv6 access-group *ACLname*

no ipv6 access-group *ACLname*

Parameters

ACLname

Specifies the name of the standard or extended IPv6 access list.

Modes

Overlay gateway configuration mode

Usage Guidelines

This command is supported in overlay-policy maps applied for overlay gateway.

You can apply an ACL to multiple overlay-policy-map stanzas.

To remove an ACL from a stanza, enter the **no** form of this command.

Examples

The following example configures an IPv6 ACL and an overlay class map. Then the policy map is created and a stanza (#10) is added. This stanza uses the class map "tunnel-group-1" to identify the gateway and specifies the IPv6 ACL "fooIpv6" on the flows within the tunnel. Finally there is a creation of the overlay gateway "gw2" and the overlay policy is applied, using the **overlay-service-policy in** command . The policy map can also applied to the overlay-transit (using the same command).

```
device# configure terminal
device(config)# ipv6 access-list extended fooIpv6
device(conf-ip6acl-ext)# seq 10 permit ipv6 host 2000::200:2 any count log
device(conf-ip6acl-ext)# seq 20 permit ipv6 host 2000::100:2 any count log
device(conf-ip6acl-ext)# seq 50000 ipv6 any any count log
device(conf-ipacl-ext)# exit

device(config)# overlay-class-map tunnel-group-1
device(config-overlay-classmap-tunnel-group-1)# seq 10 match source 1.1.1.1 destination 3.3.3.3
device(config-overlay-classmap-tunnel-group-1)# exit

device(config)# overlay-policy-map fooMap
(config-overlay-policymap-fooMap)# seq 10 overlay-class tunnel-group-1
device(config-overlay-policymap-class-tunnel-group-1) #ipv6 access-group fooIpv6
device(config-overlay-policymap-class-tunnel-group-1)# exit
device(config-overlay-policymap-fooMap)# exit

device(config)# overlay-gateway gw2
device(config-overlay-gw-gw2)# type layer2-extension
device(config-overlay-gw-gw2)# ip interface Loopback 1
device(config-overlay-gw-gw2)# map vni auto
device(config-overlay-gw-gw2)# overlay-service-policy in fooMap
device(config-overlay-gw-gw2)# site site_2
device(config-site-site_2)# ip address 1.1.1.1
device(config-site-site_2)# extend vlan add 50,60,70
device(config-site-site_2)# activate
device(config-overlay-gw-gw2)# exit
```

History

Release version	Command history
17s.1.00	This command was introduced, for security ACLs.
17s.1.01	This Overlay Services version of this command was introduced.

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 a **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using a **no access-group** command.

ATTENTION

When this command is used for VXLAN overlay gateway services, the mask for destination and source IP addresses must not exceed 64.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.01	Updated the Usage Guidelines regarding the use of this command for VXLAN overlay gateway services.

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 253 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

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.

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 0/1
device(conf-if-eth-0/1)# 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(config)# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
!
```

History

Release version	Command history
17s.1.01	This command was introduced.

ipv6 anycast-gateway-mac

Configures an IPv6 anycast-gateway MAC address, which is used as a gateway MAC address for hosts.

Syntax

ipv6 anycast-gateway-mac { **default-mac** | *MAC-address* }

no ipv6 anycast-gateway-mac

Command Default

The default IPv6 MAC address is used.

Parameters

default-mac
Specifies the default IPv6 MAC address, 02e0.5200.0200.

MAC-address
A user-specified IPv6 MAC address.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to delete a configured MAC address and revert to the default.

The default MAC address is obtained from a range of locally administered MAC addresses, and it is assumed not to conflict with other MAC addresses.

Examples

To enable configuration of a default IPv6 anycast-gateway MAC address:

```
device# configure terminal
device(config)# ipv6 anycast-gateway-mac default-mac
```

To configure a user-specified IPv6 anycast-gateway MAC address:

```
device# configure terminal
device(config)# ipv6 anycast-gateway-mac 000a.000b.000c
```

To verify the above in the running configuration:

```
device# show running-config
!
iv6p anycast-gateway-mac 000a.000b.000c
!
```

History

Release version	Command history
17s.1.01	This command was introduced.

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

The following example configures an IPv6 DHCP Relay address on a Ve interface.

```
device# configure terminal
device(config)# interface ve 100
device(config-Ve-100)# ipv6 dhcp relay address 2001::1122:AABB:CCDD:3344 use-vrf blue
```

The following example configures an IPv6 DHCP Relay address on an interface.

```
device# configure terminal
(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ipv6 dhcp relay address fe80::224:38ff:febb:e3c0  interface ethernet 0/4
```

History

Release version	Command history
17s.1.00	This command was introduced.

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# configure terminal
device(config)# ipv6 dns domain-name mycompany.com
device(config)# ipv6 dns name-server 2001:db8:12d:1300:240z:d0ff:fe48:4672
```

History

Release version	Command history
17s.1.00	This command was introduced.

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# configure terminal
device(config)# interface ethernet 0/5
device(conf-int-eth-0/5)# ipv6 icmpv6 rate-limiting
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping enable

Enables IPv6 MLDv1 Layer 2 snooping globally.

Syntax

ipv6 mld snooping enable

no ipv6 mld snooping enable

Command Default

IPv6 MLDv1 snooping is disabled.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable IPv6 MLDv1 snooping globally.

Examples

To enable IPv6 MLDv1 snooping globally:

```
device(config)# vlan 1
device(config-vlan-1)# ipv6 mld snooping enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping fast-leave

Configures the immediate-leave feature for the groups on a specific VLAN.

Syntax

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

Command Default

This feature is disabled.

Modes

VLAN configuration mode

Usage Guidelines

This command minimizes the leave latency of group memberships on an interface, as the device does not send group-specific queries. As a result, the group entry is removed from the multicast routing table as soon as a group leave message is received. Use the **no** form of this command to restore the default.

Examples

To configure the immediate-leave feature on a VLAN:

```
device(config)# vlan 1
device(config-vlan-1)# ipv6 mld snooping fast-leave
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping last-member-query-count

Configures the IPv6 MLDv1 snooping last-member query count on a specific VLAN.

Syntax

ipv6 mld last-member-query-count *value*

no ipv6 mld last-member-query-count *value*

Parameters

value

The range is from 1 through 10. The default is 2.

Modes

VLAN configuration mode

Usage Guidelines

The last-member query count is the number of times, separated by the last-member query-response interval, that an MLD query is sent in response to a host leave message from the last known active host on the subnet. Use the **no** form of this command to restore the default.

Examples

To change the IPv6 MLDv1 snooping last-member query count from the default on a VLAN.

```
device(config)# vlan 1
device(config-vlan-1)# ipv6 mld last-member-query-count 3
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping last-member-query-interval

Configures the IPv6 MLDv1 snooping last-member query interval on a VLAN.

Syntax

ipv6 mld snooping last-member-query-interval *msec*

no ipv6 mld snooping last-member-query-interval

Parameters

msec

The range is from 100 through 2500 milliseconds. The default is 1000.

Modes

VLAN configuration mode

Usage Guidelines

The last-member query interval is the interval for the response to a query sent after a host leave message is received from the last known active host on the subnet. The group is deleted if no reports are received in this interval. This interval adjusts the speed at which messages are transmitted on the subnet. Smaller values detect the loss of a group member faster. Use the **no** form of this command to restore the default.

Examples

To configure IPv6 MLDv1 snooping last-member query interval on a VLAN:

```
device(config)# vlan 1
switch(config-vlan-1)# ipv6 mld snooping last-member-query-interval 25
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping mrouter interface

Configures a VLAN port member to be a multicast router (mrouter) port.

Syntax

ipv6 mld snooping mrouter interface { **ethernet***interface name* | **port-channel** *number*}

no ipv6 mld snooping mrouter interface { **ethernet***interface name* | **port-channel** *number*}

Parameters

ethernet*interface name*
Specifies the Ethernet interface name.

port-channel*number*
Specifies the port-channel number.

Modes

VLAN configuration mode

Usage Guidelines

Use the **no** form of this command to disable the VLAN port member from being an mrouter port.

Examples

To configure a VLAN port member to be an mrouter port:

```
switch(config)# vlan 1
switch(config-vlan-1)# ipv6 mld snooping interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping querier enable

Activates or deactivates IPv6 MLDv1 Layer 2 multicast snooping querier functionality for a VLAN.

Syntax

ipv6 mld snooping querier enable

no ipv6 mld snooping querier enable

Modes

VLAN configuration mode

Usage Guidelines

Use the **no** form of this command to deactivate this functionality.

Examples

To enable MLD snooping querier functionality on a VLAN:

```
device(config)# vlan 1
device(config-vlan-1)# ipv6 mld snooping querier enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping robustness-variable

Configures a value to compensate for packet loss in congested networks.

Syntax

ipv6 mld snooping robustness-variable *value*

no ipv6 mld snooping robustness-variable

Parameters

value

The range is from 2 through 10. The default is 2.

Modes

VLAN configuration mode

Usage Guidelines

This value determines the number of general MLD snooping queries that are sent before a multicast address is aged out for lack of a response. Use the **no** form of this command to restore the default.

Examples

To change the robustness variable from the default on a VLAN:

```
device(config)# vlan 1
device(config-vlan-1)# ipv6 mld snooping robustness-variable 7
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping static-group interface

Configures IPv6 MLDv1 Layer 2 multicast static IPv6 groups on an interface for a VLAN.

Syntax

ipv6 mld snooping static-group interface *group-ipv6-address***interface***interface*

ipv6 mld snooping static-group interface

Parameters

group-ipv6-address
A multicast address to be joined.

interface
An Ethernet or port-channel interface.

Modes

VLAN configuration mode

Usage Guidelines

Use the **no** form of this command to remove the static-group configuration on an interface for a VLAN.

Examples

To configure multicast static IPv6 groups on an Ethernet interface for a VLAN:

```
device(config)# vlan 1
device(config-vlan-1)# ipv6 mld static-group ff1e::1 interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping startup-query-count

Configures the IPv6 MLDv1 number of queries that are separated by the startup query interval.

Syntax

ipv6 mld snooping startup-query-count *value*

no ipv6 mld snooping startup-query-count

Parameters

value

The range is from 1 through 10. The default is 1.

Modes

VLAN configuration mode

Usage Guidelines

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

Examples

To change the startup query count on a VLAN:

```
device(config)# vlan 1
device(config-Vlan-1)# ipv6 mld startup-query-count 5
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mld snooping startup-query-interval

Configures the IPv6 MLDv1 startup query interval.

Syntax

ipv6 mld snooping startup-query-interval *value*

no ipv6 mld snooping startup-query-interval

Command Default

This feature is disabled.

Parameters

value

The range is from 1 through 450. The default is 1.

Modes

VLAN configuration mode

Usage Guidelines

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

Examples

To change the startup query interval on a VLAN:

```
device(config)# vlan 1
switch(config-vlan-1)# ipv6 mld startup-query-interval 4
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 mtu

Sets the IPv6 maximum transmission unit (MTU) on a specified interface.

Syntax

ipv6 mtu *size*

no ipv6 mtu

Command Default

IPv6 MTU size is 1500 bytes.

Parameters

size

Specifies the size of an interface IPv6 MTU. The range is from 1300 through 9194 bytes.

Modes

Interface configuration mode

Usage Guidelines

If the interface is part of a VE, change the IPv6 MTU only at the VE interface and not at the physical port. All member ports of a VE inherit the VE-interface IPv6 MTU value.

Use the **no ipv6 mtu** command to revert the IPv6 MTU size to the default value.

Examples

On a specified Ethernet interface, the following example sets the IPv6 MTU to 2000 bytes.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ipv6 mtu 2000
```

The following example changes the IPv6 MTU for a VE.

```
device# configure terminal
device(config)# interface ve 103
device(config-if-Ve-103)# ipv6 mtu 2000
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/2
conf-if-eth-0/2)# ipv6 nd cache expire 2500
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified to reflect the default timeout change from 14400 to 1500 seconds.

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 0/1
device(conf-if-eth-0/1)# ipv6 ospf active
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 ospf area

Enables OSPFv3 on an interface.

Syntax

ipv6 ospf area *area-id* | *ip-addr*

no ipv6 ospf area

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Modes

Interface subtype configuration mode

Usage Guidelines

When this command is used, 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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 a specified OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ipv6 ospf area 0
device(conf-if-eth-0/1)# ipv6 ospf authentication spi 512 esp null hmac-sha1 key
abcef12345678901234fedcba098765432109876
```

The following example enables AH and HMAC-MD5 on a specified 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/4
device(conf-if-eth-0/4)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 ospf cost

Configures cost for a specific OSPFv3 interface.

Syntax

ipv6 ospf cost *value*

no ipv6 ospf cost

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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 0/1
device(conf-if-eth-0/1)# ipv6 ospf dead-interval 80
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535 seconds. The default is 10 seconds.

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 0/1
device(conf-if-eth-0/1)# ipv6 ospf hello-interval 20
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 ospf hello-jitter

Sets the allowed jitter between HELLO packets.

Syntax

ipv6 ospf hello-jitter *interval*

no ipv6 ospf hello-jitter

Parameters

jitter

Allowed interval between hello packets.Valid values range from 1 through 50 percent (%). The default is 10%.

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.

The **no** form of the command restores the defaults.

Examples

The following example sets the hello jitter to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ipv6 ospf hello-jitter 20
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# ipv6 ospf instance 35
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

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** 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 0/1
device(conf-if-eth-0/1)# no ipv6 ospf mtu-ignore
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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 0/1
device(conf-if-eth-0/1)# ipv6 ospf retransmit-interval 8
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# ipv6 ospf suppress-linklsa
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds. The default is 1 second.

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 0/1
device(conf-if-eth-0/1)# ipv6 ospf transmit-delay 25
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 policy route-map

Enables the IPv6 route map.

Syntax

ipv6 policy route-map *map-name*

no ipv6 policy route-map *map-name*

Command Default

The IPv6 route map is not enabled.

Parameters

map-name

Specifies the name of the route map.

Modes

Interface configuration mode

Virtual interface configuration mode

Usage Guidelines

The **no** form of the command disables the IPv6 route map.

Examples

The following example enables the IPv6 route map 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 0/1
device(conf-if-eth-0/1)# ipv6 policy route-map test-route
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 a 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 0/1
device(conf-if-eth-0/1)# ipv6 prefix-list route1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* **in**

no ipv6 receive access-group *acl-name* **in**

Command Default

No receive-path ACLs are applied.

Parameters

acl-name
: Specifies the name of the standard or extended IP access list.

in
: Specifies ingress traffic.

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 two receive-path ACLs to a device, as follows:

- One IPv4 receive-path ACL
- One IPv6 receive-path ACL

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 in
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*]

ipv6 route *dest-ipv6-prefix*/*prefix-length link-local-next-hop-ipv6-address* [**ve** *ve-id*] [*metric*] [**distance** *number*] [**tag** *tag-number*]

ipv6 route *dest-ipv6-prefix*/*prefix-length link-local-next-hop-ipv6-address* [**ethernet** *slot/port*] [*metric*] [**distance** *number*] [**tag** *tag-number*]

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* [**ve** *ve-id*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length link-local-next-hop-ipv6-address* [**ethernet** *slot/port*]

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. The slot number must be 0 if the device has no slots.

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 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.

The IPv6 prefix length must be 64 or greater for an SLX switch.

Examples

The following example creates an IPv6 static route for a destination network with the prefix 2001:DB8::0/64 and a next-hop gateway with the global address 2001:DB8:0:ee44::1.

```
device# configure terminal
device(config)# ipv6 route 2001:DB8::0/64 2001:DB8:0:ee44::1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

The IPv6 prefix length must be 64 or greater for an SLX switch.

Examples

The following example creates an IPv6 static route to IPv6 2001:DB8::0/64 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::0/64 next-hop-vrf partners 2001:DB8:0:ee44::1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The slot number must be 0 for devices that do no have slots.

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.

The IPv6 prefix length must be 64 or greater for an SLX switch.

Examples

The following example creates a primary route to all 2001 : DB8 : : 0/64 destinations through virtual interface (ve) 3. The primary route has the default cost metric of 1. The example also creates an alternative null route with a higher cost metric (2) to drop packets when the primary route is not available.

```
device# configure terminal
device(config)# ipv6 route 2001 : DB8 : : 0/64 fe80::1 ve 3
device(config)# ipv6 route 2001 : DB8 : : 0/64 null 0 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **null** *interface-name*] [**interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

no ipv6 route static bfd *dest-ipv6-address source-ipv6-address*

Command Default

BFD is not configured for an IPv6 static route.

Parameters

dest-ipv6-address
Specifies the IPv6 address of the 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.

null *interface-name*
Drops packets with this destination.

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 500.

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 500.

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

Address-family IPv6 unicast VRF configuration mode

Global configuration mode

Usage Guidelines

The **interval** *transmit-time* and **min-rx** *receive-time* variables are the intervals desired by the local device. The actual values in use will be the negotiated values.

For single-hop static BFD sessions, timeout values are optional because all required information is available from the outgoing interface. For multihop BFD sessions, if the configured **interval** and **min-rx** parameters conflict with those of an existing session, the lower values are used.

If you configure a neighbor IPv6 address and a source IPv6 address that already exist in BFD, BFD overwrites the existing interval values and multiplier for the IPv6 addresses with the new values, on behalf of the static module.

Static BFD can be configured without configuring a static route to configure a BFD session. This is especially useful on BFD neighbors when they have reachability from other neighbors via OSPF or BGP. You must configure different BFD sessions for each ECMP path with the corresponding interface IP as the source IPv6 address.

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* and *interface-name* parameters are mandatory because the link-local address can be the same on multiple interfaces.

The **no** form of the command removes the configured BFD IPv6 static route.

Examples

The following 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
```

The following example configures a BFD session on an IPv6 static route in a nondefault VRF instance.

```
device# configure terminal
device(config)# vrf orange
device(config-vrf-orange)# address-family ipv6 unicast
device(vrf-orange-ipv6-unicast)# ipv6 route static bfd fe70::a fe60::b ve 10 interval 1000 min-rx 2000
multiplier 20
```

History

Release version	Command history
17s.1.00	This command was introduced.

ipv6 route static bfd holdover-interval

Sets the time interval for which Bidirectional Forwarding Detection (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 *time*

Parameters

time

Specifies BFD holdover interval in seconds. Valid values range from 1 through 30. The default is 0.

Modes

Address-family IPv6 unicast VRF configuration mode

Global configuration mode

Usage Guidelines

If the BFD session is restored within the specified time interval, no down notification is sent.

Use the **ipv6 route static bfd holdover-interval** command in global configuration mode to set the BFD holdover interval globally for static routes.

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 for IPv6 static routes to 25.

```
device# configure terminal
device(config)# ipv6 route static bfd holdover-interval 25
```

The following example removes the configured BFD holdover interval for IPv6 static routes for a nondefault VRF instance.

```
device# configure terminal
device(config)#)# vrf orange
device(config-vrf-orange)#)# address-family ipv6 unicast
device(vrf-orange-ipv6-unicast)# no ipv6 route static bfd holdover-interval
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 virtual Ethernet (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 Virtual Ethernet 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/6
device(conf-if-eth-0/6)# ipv6 address 2001:2019:8192::125/64
device(conf-if-eth-0/6)# ipv6 vrrp-group 18
device(config-vrrp-group-18)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

Commands K - M

key

Specifies a text string to use as a shared secret between a device and a Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

key *shared_secret*

no key

Command Default

The default value is "sharedsecret".

Parameters

shared_secret

Specifies a text string to use as the shared secret between the device and the RADIUS server. The valid string length is from 8 through 40 characters. 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 configuration of an empty string.

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

Examples

The following example shows how to configure the text string "new#radius*secret" as the shared secret to use 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"
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

keypair

Associates a cryptograhic keypair with a trustpoint for security protocol exchanges for applications.

Syntax

keypair *key_label*

no keypair

Parameters

key_label

Specifies a keypair label.

Modes

Trustpoint configuration mode

Usage Guidelines

Use the **no** form of the command to remove the trustpoint keypair configuration.

Examples

The following example shows how to associate the keypair labeled k1 with a trustpoint named t1.

```
device# configure terminal
device(config)# crypto ca trustpoint t1
device(config-ca-t1)# keypair k1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

This command is not supported on static or dynamic trunks.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

For trunks, the default value is the **short** timeout.

For standard LAGs, the default value is the **long** 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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ldap-server host

Configures an LDAP-server host.

Syntax

ldap-server host { *ipaddr* | *FQDN* } [**use-vrf** *vrf-name*]

no ldap-server host { *ipaddr* | *FQDN* } [**use-vrf** *vrf-name*]

Command Default

- Timeout: 5 seconds
- Port: 389
- Retries: 5

Parameters

ipaddr | *FQDN*
Specifies the IPv4 address or Fully Qualified Domain name of the Active Directory (AD) server. IPv6 is supported for Windows 2008 AD server only. The maximum supported length for the LDAP host name is 40 characters.

use-vrf *vrf-name*
Specifies a VRF though which to communicate with the LDAP server. See the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

Use this command to set up a connection to the Lightweight Directory Access Protocol (LDAP) server host or modify an existing configuration. A maximum of 5 LDAP servers can be configured on a device.

Enter **no ldap-server host** to delete the server configuration.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

The following example adds an LDAP server on port 489 with retries set to three and the timeout set to 5 seconds.

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# basedn security.example.com
device(config-host-10.24.65.6/mgmt-vrf)# port 489
device(config-host-10.24.65.6/mgmt-vrf)# retries 3
device(config-host-10.24.65.6/mgmt-vrf)# timeout 5
```

To delete an LDAP server:

```
device# configure terminal
device(config)# no ldap-server host 10.24.65.6
```

History

Release version	Command history
17s.1.00	This command was added.

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# configure terminal
device(config)# ldap-server maprole group Administrator role admin
```

To remove the mapping:

```
device# configure terminal
device(config)# no ldap-server maprole group Administrator
```

History

Release version	Command history
17s.1.00	This command was added.

license eula

Enables the user to accept or decline the EULA for a licensed feature set.

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 wants to use the unlicensed feature set.

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 Advanced Features Self Authenticated Upgrade (SAU) license when the EULA is accepted. The Advanced Features SAU license is supported on the SLX 9140 and SLX 9240 devices.

NOTE

The Network Packet Broker (NPB) feature functionality is part of the Advanced Features SAU license.

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 Advanced Features SAU license.

```
device# license eula accept ADVANCED_FEATURES
2016/12/05-13:35:00, [SEC-1120], 64,, 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 the Advanced Features SAU license.

```
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
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	The NPB feature functionality is introduced as a part of the Advanced Features SAU license.
17s.1.02c	Rebranded from Brocade to Extreme.

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.

This command is not available on the standby management module.

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
!
```

History

Release version	Command history
17s.1.00	This command was introduced.

link-fault-signaling rx

Enables or disables ingress link-fault signaling (LFS) at device or interface level.

Syntax

link-fault-signaling rx { **off** | **on** }

no link-fault-signaling

Command Default

LFS is enabled.

Parameters

off

Disables ingress LFS at device or interface level.

on

Enables ingress LFS at device or interface level.

Modes

Global configuration mode

Interface subtype configuration mode

Usage Guidelines

This command is supported both in default system mode and network packet broker (NPB) mode.

When LFS is on, if there is an ingress link fault, the affected interface is brought down. When LFS is off, if the PHY-MAC link is up, the interface stays up—even if there is an ingress link fault.

You cannot override the egress LFS setting. If there is an egress link fault, the affected interface is brought down.

You can configure LFS settings both globally and at interface-level. Local LFS settings override the global setting.

To restore the default setting of LFS enabled, enter **no link-fault-signaling**.

Examples

The following example changes the global ingress LFS setting from **on** to **off**.

```
device# configure terminal
device(config)# link-fault-signaling rx off
```

The following example resets the global ingress LFS setting to the default **on**.

```
device# configure terminal
device(config)# no link-fault-signaling
```

The following example sets an interface ingress LFS setting to **off**, overriding the global setting.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# link-fault-signaling rx off
```

The following example sets an interface ingress LFS setting to configured on, overriding the global setting.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# link-fault-signaling rx on
```

The following example sets an interface ingress LFS setting to default on—but able to be overridden by a global **link-fault-signaling rx off**.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no link-fault-signaling
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

load-balance (default mode)

Configures the LAG load balancing settings.

Syntax

load-balance { **dst-mac-vid** | **src-mac-vid** | **src-dst-mac-vid** | **src-dst-ip** | **src-dst-ip-mac-vid** | **src-dst-ip-port** | **src-dst-ip-mac-vid-port** }

no load-balance

Command Default

The default setting is **src-dst-ip-mac-vid-port**.

Parameters

dst-mac-vid
Specifies that the distribution is based on the destination MAC address and outer VLAN ID (VID).

src-mac-vid
Specifies that the distribution is based on the source MAC address and VID.

src-dst-mac-vid
Specifies that the distribution is based on the the source and destination MAC addresses and VID.

src-dst-ip
Specifies that the distribution is based on the the source and destination IPv4 or IPv6 addresses.

src-dst-ip-mac-vid
Specifies that the distribution is based on the source and destination IPv4 or IPv6 and MAC addresses; and the VID.

src-dst-ip-port
Specifies that the distribution is based on the source and destination IPv4 or IPv6 addresses and TCP port.

src-dst-ip-mac-vid-port
Specifies that the distribution is based on the source and destination IPv4 or IPv6 and MAC addresses, VID, and port.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to return to the default setting.

Examples

The following example specifies destination MAC address and VID-based load balancing.

```
device# configure terminal
device(config)# load-balance dst-mac-vid
```

History

Release version	Command history
17s.1.00	This command was introduced.

load-balance (NPB mode)

Configures the LAG load balancing settings, in Network Packet Broker (NPB) mode.

Syntax

load-balance { **dst-mac-vid** | **src-mac-vid** | **src-dst-mac-vid** | **src-dst-ip** | **src-dst-ip-mac-vid** | **src-dst-ip-port** | **src-dst-ip-mac-vid-port** }

no load-balance

Command Default

The default setting is **src-dst-ip-mac-vid-port**.

Parameters

dst-mac-vid
(Not supported in NPB mode) Specifies that the distribution is based on the destination MAC address and outer VLAN ID (VID).

src-mac-vid
(Not supported in NPB mode) Specifies that the distribution is based on the source MAC address and VID.

src-dst-mac-vid
Specifies that the distribution is based on the source and destination MAC addresses; and VID.

src-dst-ip
Specifies that the distribution is based on the source and destination IPv4 or IPv6 address.

src-dst-ip-mac-vid
Specifies that the distribution is based on the source and destination IPv4 or IPv6 addresses, MAC address, and VID.

src-dst-ip-port
Specifies that the distribution is based on the source and destination IPv4 or IPv6 addresses and TCP or UDP destination port.

src-dst-ip-mac-vid-port
Specifies that the distribution is based on the source and destination IPv4 or IPv6, MAC address, VID, and TCP or UDP destination port.

Modes

Global configuration mode

Usage Guidelines

The only type of load balancing supported in NPB mode is symmetric load-balance hashing.

In NPB mode, the VID component of keywords is ignored.

Use the **no** form of this command to return to the default setting.

Examples

The following example specifies that the distribution is based on source and destination MAC addresses and VLAN ID.

```
device# configure terminal
device(config)# load-balance src-dst-mac-vid
```

History

Release version	Command history
17s.1.00	The default system mode version of this command was introduced.
17s.1.02	The Network Packet Broker (NPB) version of this command was introduced.

local-as

Specifies the BGP autonomous system number (ASN) where the device resides.

Syntax

local-as *num*

no local-as *num*

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

The following example assigns a separate local AS number.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 777
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

log-dampening-debug

Logs dampening debug messages.

Syntax

log-dampening-debug

no log-dampening-debug

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command disables the logging of dampening debug messages.

Examples

The following example logs dampening debug messages.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# log-dampening-debug
```

History

Release version	Command history
17s.1.00	This command was introduced.

log-shell

Controls the remote logging of SLXVM Linux shell command activities.

Syntax

log-shell start | **status** | **stop**

Command Default

By default, supported devices log 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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

logging syslog-client

Configure various parameters used by syslog clients.

Syntax

logging syslog-client localip { CHASSIS_IP }

Parameters

CHASSIS_IP

Uses the Chassis IP address as source IP address in the IP header of syslog messages generated by this device.

Modes

Global configuration mode

Examples

Example command for using the chassis IP as the source IP in the IP header of syslog messages, generated by this device.

```
device# configure terminal
device(config)# logging syslog-client localip CHASSIS_IP
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

logging syslog-server

Configures a switch to forward system messages to specified syslog servers.

Syntax

logging syslog-server *ip_address* [**secure**] [**port** *port-num*] [**use-vrf** *vrf-name*]

no logging syslog-server *ip_address* [**secure**] [**port** *port-num*] [**use-vrf** *vrf-name*]

Parameters

ip_address
Specifies the IP address of the syslog server in IPv4 or IPv6 format.

secure
Configures a secure default (port 514) or specified nondefault syslog server port. A secure port number with default values is not shown in the Extreme SLX-OS database.

port *port-num*
Specifies a nondefault port. The port range is from 1 through 65535.

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 one or more specified servers. You can configure up to four servers.

A secure port number with default values is not shown in the database.

The **certutil import syslogca** command is required for secure syslog to be fully functional.

You can configure up to four syslog servers; this includes all VRFs. You must execute the command for each server.

Use the **no logging syslog-server** command with the optional **use-vrf** keyword to remove the specified IP address 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 server IPv4 address and specify a VRF with a secure nondefault port, and confirm the configuration:

```
device# configure terminal
device(config)# logging syslog-server 192.168.163.233 use-vrf myvrf secure port 1999
device(config-syslog-server-192.168.163.233/myvrf)# do show running-config logging syslog-server
logging syslog-server 192.168.163.233 use-vrf myvrf
secure port 1999
```

To remove a configured syslog server:

```
device# configure terminal
device(config)# no logging syslog-server 192.168.163.233
```

To remove a syslog nondefault server port and confirm the configuration:

```
device# configure terminal
device(config)# no logging syslog-server 10.17.17.203 secure port 1999
device(config)# do show running-config logging syslog-server
logging syslog-server 10.17.17.203
secure
```

History

Release version	Command history
17s.1.00	This command was introduced.

logical-interface

Creates a logical interface to an Ethernet or port-channel interface, and binds a logical interface to a bridge domain.

Syntax

logical-interface { **ethernet** *0/port* | **port-channel** *num* }

no logical-interface { **ethernet** *0/port* | **port-channel** *num* }

Command Default

No interface is bound to the bridge domain.

Parameters

ethernet *o/port*
Specifies the port number for the Ethernet interface.

port-channel *num*
Specifies an instance ID for a port-channel logical interface.

Modes

Interface subtype configuration mode

Bridge-domain configuration mode

Usage Guidelines

The attachment circuit end-points (logical interfaces) bound to a bridge domain can be either regular Ethernet interfaces or LAG trunks (port channels).

A logical interface with a VLAN must be created by using the **logical-interface** command in interface configuration mode before it can be bound to a bridge domain.

The **no** version of the command removes the logical interface from the bridge domain configuration.

Examples

The following example shows how to create a logical Ethernet interface instance ID (0/5.10) and bind to bridge domain 4.

```
device# configure terminal
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# logical-interface ethernet 0/5.10
device(conf-if-eth-lif-0/5.10)# vlan 50
device(conf-if-eth-lif-0/5.10)# exit
device(conf-if-eth-0/5)# exit
device(config)# bridge-domain 4
Succeeded
device(config-bridge-domain-4)# logical-interface ethernet 0/5.10
```

The following example shows how to bind a logical port-channel interface instance ID (2.200) to bridge domain *4*.

```
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 0/3.100
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# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 0/3.100
 Error: LIF already Binded
```

History

Release version	Command history
17s.1.00	This command was introduced.

loopback phy

Implements internal loopback on a physical or port-channel interface.

Syntax

loopback phy

no loopback phy

Command Default

Internal loopback is not implemented.

Modes

Ethernet interface configuration mode

Port-channel configuration mode

Usage Guidelines

To disable internal loopback on an interface, use the **no** form of this command.

Examples

The following example implements internal loopback on a physical interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# loopback phy
```

The following example disables internal loopback on a physical interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# no loopback phy
```

The following example implements internal loopback on a port-channel interface.

```
device# configure terminal
device(config)# interface port-channel 20
device(config-Port-channel-20)# loopback phy
```

History

Release version	Command history
18s.1.01	This command was introduced.

mac access-group (general)

Applies rules specified in a MAC access control list (ACL) to traffic entering or exiting an interface.

Syntax

mac access-group *ACLname* { **in** | **out** } [**switched** | **routed**]

no mac access-group *ACLname* { **in** | **out** } [**switched** | **routed**]

Parameters

ACLname
Specifies the name of the standard or extended MAC access list.

in
Specifies to filter inbound packets only.

out
Specifies to filter outbound packets only.

switched
Filter only switched traffic. This parameter is not valid for the management interface.

routed
Filter only routed traffic. This parameter is not valid for the management interface.

Modes

Interface-subtype configuration mode

Usage Guidelines

You can apply a maximum of six ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- (VLANs only) One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- (VEs only) One egress IPv4 ACL
- One ingress IPv6 ACL
- (VEs only) One egress 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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

mac access-group (overlay)

Applies rules specified in a MAC ACL to traffic entering or traversing a tunnel.

Syntax

mac access-group *ACLname*

no mac access-group *ACLname*

Parameters

ACLname

Specifies the name of the standard or extended MAC access list.

Modes

Overlay gateway configuration mode

Usage Guidelines

This command is supported in overlay-policy maps applied for overlay gateway.

You can apply an ACL to multiple overlay-policy-map stanzas.

To remove an ACL from a stanza, enter the **no** form of this command.

Examples

The following example configures a MAC ACL and an overlay class map. Then the policy map is created and a stanza (#10) is added. This stanza uses the class map "tunnel-group-1" to identify the gateway and specifies the MAC ACL "fooL2" on the flows within the tunnel. Finally there is a creation of the overlay gateway "gw2" and the overlay policy is applied, using the **overlay-service-policy in** command . The policy map can also applied to the overlay-transit (using the same command).

```
device# configure terminal
device(config)# mac access-list extended fooL2
device(conf-macl-ext)# seq 10 permit host 0000.4400.0002 any count
device(conf-macl-ext)# seq 20 permit host 0000.ab00.0002 any count
device(conf-macl-ext)# seq 50000 deny any any count
device(conf-macl-ext)# exit

device(config)# overlay-class-map tunnel-group-1
device(config-overlay-classmap-tunnel-group-1)# seq 10 match source 1.1.1.1 destination 3.3.3.3
device(config-overlay-classmap-tunnel-group-1)# exit

device(config)# overlay-policy-map fooMap
(config-overlay-policymap-fooMap)# seq 10 overlay-class tunnel-group-1
device(config-overlay-policymap-class-tunnel-group-1) #fooL2
device(config-overlay-policymap-class-tunnel-group-1)# exit
device(config-overlay-policymap-fooMap)# exit

device(config)# overlay-gateway gw2
device(config-overlay-gw-gw2)# type layer2-extension
device(config-overlay-gw-gw2)# ip interface Loopback 1
device(config-overlay-gw-gw2)# map vni auto
device(config-overlay-gw-gw2)# overlay-service-policy in fooMap
device(config-overlay-gw-gw2)# site site_2
device(config-site-site_2)# ip address 1.1.1.1
device(config-site-site_2)# extend vlan add 50,60,70
device(config-site-site_2)# activate
device(config-overlay-gw-gw2)# exit
```

History

Release version	Command history
17s.1.00	This command was introduced, for security ACLs.
17s.1.01	This Overlay Services version of this command was introduced.

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.

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# configure terminal
device(config)# mac access-list extended mac1
```

The following example deletes a MAC extended ACL named mac1.

```
device# configure terminal
device(config)#  no mac access-list extended mac1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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# configure terminal
device(config)# mac access-list standard mac1
device(conf-macl-std)#
```

The following command deletes a MAC standard ACL named mac1.

```
device# configure terminal
device(config)# no mac access-list standard mac1
```

History

Release version	Command history
17s.1.00	This command was introduced.

mac-address-table

Sets the aging time, sets mac-move parameters, enables conversational MAC learning, and adds static addresses to the MAC address table.

Syntax

mac-address-table aging-time *aging-time*

no mac-address-table aging-time

mac-address-table aging-time conversational *conversational-aging-time*

no mac-address-table aging-time conversational

mac-address-table learning-mode conversational

no mac-address-table learning-mode conversational

mac-address-table mac-move { **detect** | **limit** *max-mac-moves* }

no mac-address-table mac-move limit

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.

Conversational aging time is 300 seconds.

Conversational MAC learning is disabled.

The MAC-move limit is 20 moves.

Parameters

aging-time *aging-time*

Specifies the time in seconds that a learned MAC address will persist after the last update. If the aging time is set to zero (0), it means that aging is disabled. Otherwise, values range from 60 through 100000. The default is 1800 seconds.

conversational *conversational-aging-time*

Configures an aging time for conversational MAC addresses learned by destination address (DA). If the aging time is set to zero (0), it means that aging is disabled. Otherwise, values range from 60 through 100000. The default is 300 seconds.

learning-mode conversational
Enables conversational MAC learning, rather than the default dynamic learning mode.

mac-move
Configures MAC-move detection.

detect
Enables MAC-move detection.

limit *max-mac-moves*
Specifies the MAC-move limit. Thre range is 5 through 500 moves. The default is 20 moves.

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 restore the default MAC aging time of 1800 seconds, use the **no mac-address-table aging-time** option.

To restore the default conversational MAC aging time of 300 seconds, use the **no mac-address-table aging-time conversational** option.

To disable conversational MAC learning and restore default dynamic MAC learning, use the **no mac-address-table learning-mode conversational** option.

To restore the default MAC-move limit of 20 moves, use the **no mac-address-table mac-move limit** option.

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 sets the aging time to 600 seconds.

```
device# configure terminal
device(config)# mac-address-table aging-time 600
```

The following example sets the aging time for conversational MAC addresses to 600 seconds.

```
device# configure terminal
device(config)# mac-address-table aging-time conversational 600
```

The following example enables conversational MAC learning.

```
device# configure terminal
device(config)# mac-address-table learning-mode conversational
```

The following example restores aging time to its default value of 1800 seconds.

```
device# configure terminal
device(config)# no mac-address-table aging-time
```

The following example disables aging time by setting its value to 0.

```
device# configure terminal
device(config)# mac-address-table aging-time 0
```

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
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified, changing the default aging time from 300 seconds to 1800 seconds.

mac-address-table mac-move detect

Enables MAC-move detection on the switch.

Syntax

mac-address-table mac-move detect

no mac-address-table mac-move detect

Command Default

This feature is disabled.

Modes

Global configuration mode

Usage Guidelines

MAC address moves are often caused by loops, overloading control-plane resources. When this feature is enabled, the default number of MAC-moves that are detected is 20. This limit can be changed by means of the **mac-address-table mac-move limit** command.

The **no** form of this command disables MAC-move detection.

Examples

The following example enables MAC-move detection on the switch.

```
device# configure terminal
device(config)# mac-address-table mac-move detect
```

History

Release version	Command history
17s.1.00	This command was introduced.

mac-address-table mac-move limit

Specifies the upper limit for MAC-address-moves detected—in any 10-second window—without triggering MAC-address-move resolution.

Syntax

mac-address-table mac-move limit *move_threshold*

no mac-address-table mac-move limit

Command Default

When MAC-address-move detection is enabled, by means of the **mac-address-table mac-move detect** command, and *move_threshold* is not specified, the default for *move_threshold* is 20.

Parameters

move_threshold

Specifies the number of MAC-address moves (in any 10-second window) above which the repeated-MAC-moves feature is triggered. Range is from 5 through 500. The default is 20.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command sets *move_threshold* to 20, which triggers the feature from the first MAC-address move.

Examples

The following example sets the number of MAC-moves detected without triggering MAC-address-move resolution to 10.

```
device# configure terminal
device(config)# mac-address-table mac-move limit 10
```

The following example resets the *move_threshold* to zero.

```
device# configure terminal
device(config)# no mac-address-table mac-move limit
```

History

Release version	Command history
17s.1.00	This command was introduced.

map

Specifies the map to be used for the group of remark values in the default policer remarking profile.

Syntax

map *remark-value-group map-name*

Command Default

The **police-remark-profile** command has been executed. Then, the **action** command has been executed, specifying a classification type of **color-and-cos**, **color-and-traffic-class**, or **color-and-dscp**.

Parameters

remark-value-group

Specifies the group of remark values to which the specified map applies. Choices include:

- cos-dscp
- cos-mutation
- cos-traffic-class
- dscp-cos
- dscp-traffic-class
- dscp-mutation
- traffic-class-cos
- traffic-class-dscp
- traffic-class-mutation

map-name

Specifies the map.

Modes

Policer remarking profile configuration mode

Usage Guidelines

Use this command after executing the **police-remark-profile** command and after executing the **action** command, specifying a classification type of **color-and-cos**, **color-and-traffic-class**, or **color-and-dscp**. Then, issue the **map** command to specify the map used to modify the remark values in the default policer remark profile.

Examples

The following is an example of executing the **action** command to specify the color-and-cos classification type for exceeding traffic. Then, the example shows using the **map** command to specify the maps to be included in the default policer remark profile for cos remarking for exceeding traffic. ("cm1," "ct1," and "cd1" are map names).

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color-and-cos exceed
device(police-remark-profile-color-and-cos-exceed)# map cos-mutation cm1
device(police-remark-profile-color-and-cos-exceed)# map cos-traffic-class ct1
device(police-remark-profile-color-and-cos-exceed)# map cos-dscp cd1
device(police-remark-profile-color-and-cos-exceed)# exit
```

The following is an example of executing the **action** command to specify the color-and-dscp classification type for conforming traffic. Then, the example shows using the **map** command to specify the maps to be included in the default policer remark profile for dscp remarking for conforming traffic. ("dm1," "dc1," and "dt1" are map names).

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color-and-dscp conform
device(police-remark-profile-color-and-dscp-conform)# map dscp-mutation dm1
device(police-remark-profile-color-and-dscp-conform)# map dscp-cos dc1
device(police-remark-profile-color-and-dscp-conform)# map dscp-traffic-class dt1
device(police-remark-profile-color-and-dscp-conform)# exit
```

The following is an example of executing the **action** command to specify the color-and-traffic-class classification type for exceeding traffic. Then, the example shows using the **map** command to specify the maps to be included in the default policer remark profile for traffic-class remarking for exceeding traffic. ("tm2," "tc2," and "td2" are map names).

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color-and-traffic-class exceed
device(police-remark-profile-color-and-traffic-class-exceed)# map traffic-class-mutation tm2
device(police-remark-profile-color-and-traffic-class-exceed)# map traffic-class-cos tc2
device(police-remark-profile-color-and-traffic-class-exceed)# map traffic-class-dscp td2
device(police-remark-profile-color-and-traffic-class-exceed)# exit
```

History

Release version	Command history
17s.1.00	This command was introduced.

map bridge-domain (VXLAN gateway)

Maps a bridge domain (BD) or range of BDs to a Virtual Network Identifier (VNI) or range of VNIs for a VXLAN overlay gateway.

Syntax

map bridge-domain { *vlan_id* | **vni** *vni* }

no map bridge-domain { *vlan_id* | **vni** *vni* }

Command Default

No bridge domain is mapped.

Parameters

vlan_id

Specifies a VLAN or range of VLANs. Range is from 1 through 4096.

vni *vni*

Specifies a VNI or range of VNIs. Range is from 1 through 16777215.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Use the **no** form of this command to remove the mapping.

Examples

To map a BD to a VNI:

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# map bridge-domain 10 vni 10
```

To map a range of BDs to a range of VNIs:

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# map bridge-domain 10-30 vni 10-30
```

To remove the mapping:

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# no map bridge-domain 10-30 vni 10-30
```

History

Release version	Command history
17s.1.01	This command was introduced.

map cos

Maps an ingress CoS value to an outbound CoS, DSCP, or Traffic-class value for a QoS CoS-mutation, CoS-to-DSCP, or CoS-to-traffic class map.

Syntax

map cos *cos-value* **to** { **cos** *cos-out* } | { **dscp** *dscp-out* } | { **traffic-class** *tc-value* }

no map cos *cos-value*

Command Default

The default values for QoS CoS-mutation, CoS-to-DSCP, or CoS-to-traffic class mapping.

Parameters

cos-value
Specifies the ingress CoS value. Enter an integer from 0 to 7.

cos *cos-out*
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

CoS mutation configuration mode

CoS DSCP configuration mode

CoS traffic-class configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default values.

Examples

In CoS mutation configuration mode, the following example maps an ingress CoS value to an egress CoS value.

```
device# configure terminal
device(config)# qos map cos-mutation test
device(cos-mutation-test)# map cos 1 to cos 5
```

In CoS DSCP configuration mode, the following example maps an ingress CoS value to an egress DSCP value.

```
device# configure terminal
device(config)# qos map cos-dscp test
device(cos-dscp-test)# map cos 4 to dscp 43
```

In CoS traffic configuration mode, the following example maps the ingress CoS values to a traffic class.

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(cos-traffic-class-test)# map cos 3 to traffic-class 1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

map traffic-class

Maps an ingress traffic class to an outbound traffic class, CoS, or DSCP value for a QoS traffic class-to-CoS, traffic class-to-DSCP, or traffic-class-mutation map.

Syntax

map traffic-class *traffic-class-value* **to** { **cos** *cos-value* } | { **dscp** *dscp-out* } | { **traffic-class** *tc-out* }

no map dscp *dscp-value*

Command Default

The default values for traffic class-to-CoS, traffic class-to-DSCP, or traffic-class-mutation mapping.

Parameters

traffic-class-value
Specifies the ingress traffic class value. Enter an integer from 0 to 7.

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-out*
Specifies the outbound Traffic Class value. Enter an integer from 0 to 7.

Modes

Traffic-class CoS configuration mode

Traffic-class DSCP configuration mode

Traffic-class mutation configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default values.

Examples

In traffic-class CoS configuration mode, the following example maps an ingress traffic-class value to an egress CoS value.

```
device# configure terminal
device(config)# qos map traffic-class-cos test1
device(traffic-class-cos-test1)# map traffic-class 3 to cos 7
```

In traffic-class DSCP configuration mode, the following example maps the ingress traffic-class value to a DSCP value.

```
device# configure terminal
device(config)# qos map traffic-class-dscp test1
device(traffic-class-dscp-test1)# map traffic-class 4 to dscp 55
```

In traffic-class mutation configuration mode, the following example maps the ingress traffic-class values to an egress traffic-class value.

```
device# configure terminal
device(config)# qos map traffic-class-mutation test1
device(traffic-class-mutation-test1)# map traffic-class 4 to traffic-class 0
```

History

Release version	Command history
17s.1.00	This command was introduced.

map vlan (VXLAN gateway)

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*]

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 4096. See the Usage Guidelines.

vni

Specifies the VNI (VXLAN Network Identifier) token.

vni

A single VXLAN VNI or range of VXLAN VNIs. The range is from 1 through 16777215. See the Usage Guidelines.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Note the following conditions: [

- Before using this command, first set the VXLAN overlay gateway to **layer2-extension**, by means of the **type** command, and 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, the 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.

Examples

The following example configures a manual mapping of VLANs to VNIs in "gateway1".

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

The following example configures an automatic mapping of VLANs to VNIs in "gateway1".

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# map vlan vni auto
```

History

Release version	Command history
17s.1.01	This command was introduced.

map vni auto (VXLAN gateway)

Configures an automatic mapping of VLANs/bridge domains (BDs) to Virtual Network Identifiers (VNIs).

Syntax

map vni { **auto** }

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-gatgeway mygateway
device(config-overlay-gateway-mygateway)# map vni auto
```

The following example undoes the mapping.

```
device# configure terminal
device(config)# overlay-gatgeway mygateway
device(config-overlay-gateway-mygateway)# no map vni auto
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

class-map

Examples

The following example matches an ACL to a class map.

```
device# configure terminal
device(config)# class-map default
device(config-classmap)# match access-group class_acl
```

History

Release version	Command history
17s.1.00	This command was introduced.

match as-path

Matches an AS-path access list name in a route-map instance.

Syntax

match as-path *name*

no match as-path

Parameters

name

Name of an AS-path access list. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Enter **no match as-path** *name* to disable this feature.

You can configure up to five match AS-Path 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 as-path ABCPath
```

History

Release version	Command history
17s.1.00	This command was introduced.

match community

Configures matching based on a community access list for a route-map instance.

Syntax

match community *name*

no match community *name*

Parameters

name

Name of a community access list. The format is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Enter **no match community** *name* to disable matching based on a community list.

Examples

The following example shows how to configure matching based on a 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 community ABCPath
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

You can configure up to five match extcommunity directives within a single stanza.

The **no** form of the command removes the community match statement from the configuration file.

Examples

The following example configures 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

match interface

Matches interface conditions in a route-map instance.

Syntax

match interface { **ethernet 0/***port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id* }

no match interface

Parameters

ethernet 0/*port*
Specifies the Ethernet interface. Enter a valid port number, must be 0 if the switch does not contain slots.

loopback *number*
Specifies a loopback port number. The range is from 1 through 255.

port-channel *number*
Specifies a port-channel interface. The range is from 1 through 6144.

ve *vlan_id*
Specifies the VLAN number. (Refer to the Usage Guidelines.) The range is from 1 through 4095.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to configure the interface match clause in a route-map instance. A maximum of seven interfaces is supported.

There is no restriction on the number or type of each interface specified, as long as the total is less than or equal to seven.

Examples

The following example configures a route-map that matches on an interface.

```
device# configure terminal
device(config)# route-map myintroutemap1 permit 99
device(config-route-map-myintroutemap1/permit/99)# match interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

An NPB route-map stanza can contain only one **match { ip | ipv6 | mac | uda } address acl** statement.

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 aclNPB_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_2
```

History

Release version	Command history
17s.1.01	This command was introduced.

match ip address prefix-list

Matches IPv4 address conditions in a route map instance.

Syntax

match ip address prefix-list *prefix-list-name*

no match ip address prefix-list *prefix-list-name*

Command Default

No routes are distributed based on destination network number.

Parameters

prefix-list-name

Specifies the name of an IP prefix list. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

You can configure up to five match address prefix-list directives within a single stanza.

Use the **no** form of this command to remove the match.

Examples

The following example matches IP routes that have addresses specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# ip prefix-list myprefixlist permit 1.2.3.0/24
device(config)# ip prefix-list myprefixlist permit 4.5.6.0/24 le 28 ge 25
device(config)# route-map extComRmap permit 10
device(config-route-map-extComRmap)# match ip address prefix-list myprefixlist
```

History

Release version	Command history
17s.1.00	This command was introduced.

match ip next-hop prefix-list

Matches IP next-hop match conditions in a route-map instance.

Syntax

match ip next-hop prefix-list *name*

no match ip next-hop

Parameters

prefix-list *name*

Specifies a IP prefix list. Values range from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify an IP next-hop match clause in a route-map instance.

You can configure up to five match next-hop prefix-list directives within a single stanza.

The **no** form of the command removes the **match ip next-hop prefix-list** *prefix-list-name*entry.

Examples

The following example matches IP routes that have the next hop specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-ExtComRmap)# match ip next-hop prefix-list myprefixlist
```

History

Release version	Command history
17s.1.00	This command was introduced.

match ip route-source prefix-list

Matches IP route-source match conditions in a route-map instance.

Syntax

match ip route-source prefix-list *name*

no match ip route-source

Parameters

prefix-list *name*

Specifies a IP prefix list. Values range from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify an IP route-source match clause in a route-map instance.

You can configure up to five match route-source prefix-list directives within a single stanza.

The **no** form of the command removes the **match ip route-source prefix-list** *prefix-list-name* entry.

Examples

The following example matches IPv6 routes that have the route source specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-ExtComRmap)# match ip route-source prefix-list myprefixlist
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

This command is supported only under Network Packet Broker (NPB).

A route-map stanza can contain only one **match { ip | ipv6 | mac |uda } address acl** statement.

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_NPB_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_NPB_01
```

History

Release version	Command history
17s.1.01	This command was introduced.

match ipv6 address prefix-list

Matches IPv6 address conditions in a route map instance.

Syntax

match ipv6 address prefix-list *prefix-list-name*

no match ipv6 address prefix-list *prefix-list-name*

Command Default

No routes are distributed based on destination network number.

Parameters

prefix-list-name

Specifies the name of an IPv6 prefix list. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

You can configure up to five match address prefix-list directives within a single stanza.

Use the **no** form of this command to remove the match.

Examples

The following example matches IPv6 routes that have addresses specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-ExtComRmap)# match ipv6 address prefix-list myprefixlist
```

History

Release version	Command history
17s.1.00	This command was introduced.

match ipv6 next-hop prefix-list

Matches IPv6 next-hop match conditions in a route-map instance.

Syntax

match ipv6 next-hop prefix-list *name*

no match ipv6 next-hop

Parameters

prefix-list *name*

Specifies a IPv6 prefix list. Values range from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify an IPv6 next-hop match clause in a route-map instance.

You can configure up to five match next-hop prefix-list directives within a single stanza.

The **no** form of the command removes the **match ipv6 next-hop prefix-list** *prefix-list-name* entry.

Examples

The following example matches IPv6 routes that have the next hop specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-ExtComRmap)# match ipv6 next-hop prefix-list myprefixlist
```

History

Release version	Command history
17s.1.00	This command was introduced.

match ipv6 route-source prefix-list

Matches IPv6 route-source match conditions in a route-map instance.

Syntax

match ipv6 route-source prefix-list *name*

no match ipv6 route-source

Parameters

prefix-list *name*

Specifies an IPv6 prefix list. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify an IPv6 route-source match clause in a route-map instance.

You can configure up to five match route-source prefix-list directives within a single stanza.

The **no** form of the command removes **match ipv6 route-source prefix-list** *prefix-list-name* entry.

Examples

The following example matches IPv6 routes that have the route source specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-ExtComRmap)# match ipv6 route-source prefix-list myprefixlist
```

History

Release version	Command history
17s.1.00	This command was introduced.

match mac address acl (NPB)

In a route map instance, matches MAC address conditions specified in a Layer 2 ACL.

Syntax

match mac address acl *acl-name*

no match ip address acl *acl-name*

Parameters

acl-name

Specifies a Layer 2 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

Route-map configuration mode

Usage Guidelines

A route-map stanza can contain only one **match { ip | ipv6 | mac | uda } address acl** statement.

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 a Layer 2 (MAC) 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) mac access-list extended acl_4
device(conf-macl-ext)# permit host 00ab.0000.0001 any count
device(conf-macl-ext)# permit host 00ab.0000.0002 any count
device(conf-macl-ext)# deny host 00ab.0000.0003 any count
device(conf-macl-ext)# exit
device(config)# route-map example3 permit 1
device(config-route-map-example3/permit/1)# match mac address acl acl_4
```

History

Release version	Command history
17s.1.01	This command was introduced.

match metric

Matches a route metric in a route-map instance.

Syntax

match metric *value*

no match metric

Parameters

value

Matches a route metric in a route-map instance. Values range from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify a route-map metric in route-map instance.

Examples

The following example configures a metric that matches on a specified value.

```
device# configure terminal
device(config)# route-map myintroutemap1 permit 99
device(config-route-map-myintroutemap1/permit/99)# match metric 8675309
```

History

Release version	Command history
17s.1.00	This command was introduced.

match protocol

Matches routes on protocol types and subtypes in a route-map instance.

Syntax

match protocol { [**static**] | [**bgp** [**external** | **internal**]] }

no match protocol

Parameters

bgp external
Matches EBGP routes.

bgp internal
Matches IBGP routes.

static-network
Matches BGP static routes. This is applicable only for BGP outbound policy.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify a route-map protocol in route-map instance.

Examples

The following example configures a protocol for matching route map.

```
device# configure terminal
device(config)# route-map myintroutemap1 permit 99
device(config-route-map-myintroutemap1/permit/99)# match protocol bgp internal
```

History

Release version	Command history
17s.1.00	This command was introduced.

match route-type

Matches a route type in a route-map instance.

Syntax

match route-type [**internal** | **type-1** | **type-2**]

no match route-type

Parameters

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

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify a route-type in route-map instance.

Examples

Typical command example

```
device# configure terminal
device(config)# route-map myintroutemap1 permit 99
device(config-route-map-myintroutemap1/permit/99)# match route-type internal
```

History

Release version	Command history
17s.1.00	This command was introduced.

match tag

Matches a route tag in a route-map instance.

Syntax

match tag *value*

no match tag

Parameters

value

Specifies a route tag and route tag value. The range of valid values is from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify a route tag in route-map instance.

Examples

Typical command example

```
device# configure terminal
device(config)# route-map myintroutemap1 permit 99
device(config-route-map-myintroutemap1/permit/99)# match tag 8675308
```

History

Release version	Command history
17s.1.00	This command was introduced.

match uda address acl

In a route-map stanza, matches conditions specified in a user-developed ACL (UDA).

Syntax

match uda address acl *acl-name*

no match uda address acl *acl-name*

Parameters

acl-name

Specifies a UDA ACL name unique among all ACLs (Layer 2, Layer 3, and UDA). 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

This command is supported only in NPB system mode.

A route-map stanza can contain only one **match { ip | ipv6 | mac | uda } address acl** statement.

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 a UDA ACL and then includes that ACL in a route-map stanza.

```
device# configure terminal
device(config)# uda access-list extended uda_acl_01
device(conf-uda-acl-ext)# permit 0x112233 0xFFFFFF 0x0a0a0001 0xFFFFFFFF 0x0a0b0001 0xFFFFFFFF
0x11223344 0xFFFFFFFF
device(conf-uda-acl-ext)# exit
device(config)# route-map example1 permit 1
device(config-route-map-example1/permit/1)# match uda address acl uda_acl_01
```

History

Release version	Command history
18s.1.00	This command was introduced.

match vrf

Specifies a non-default VRF in a route-map instance.

Syntax

match vrf *name*

no match tag

Parameters

vrf *name*

Specifies a non-default VRF. Valid values range from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

Use this command to specify a non-default VRF in a route-map instance.

Examples

Typical command example

```
device# configure terminal
device(config)# route-map myintroutemap1 permit 99
device(config-route-map-myintroutemap1/permit/99)# match VRF 8675307
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Parameters

in

Allows an AS-PATH attribute from any neighbor to impose a limit on the number of autonomous systems.

num

Specifies a value. Valid values range from 0 through 300. The default is 300.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command restores the default of 300.

Examples

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

maximum-paths (BGP)

Sets the maximum number of BGP4 and BGP4+ shared paths.

Syntax

maximum-paths *num* | **use-load-sharing**

no maximum-paths

Parameters

num

Specifies the maximum number of paths across which the device balances traffic to a given BGP destination. Valid values range is from 1 through 64. The default is 1.

use-load-sharing

Uses the maximum IP ECMP path value supported (64) 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 (64) 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 defaults.

Examples

The following example sets the maximum number of BGP4 shared paths to 8.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maximum-paths 8
```

The following example sets the maximum number of BGP4+ shared paths to 64 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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

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.

The **no** form of the command restores the defaults.

Examples

The following 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
```

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

When this command is used, 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 16777215 (0x00001 - 0x00FFFFFE).

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).

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

When this command is used, 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

max-route

Specifies the maximum number of routes allowed in the routing table per VRF instance, for an IPv4 or IPv6 VRF address family.

Syntax

max-route *value*

Command Default

If this command is not configured, the maximum allowed number of routes, 4294967295 (see Parameters), is applied. This number does not appear in a running configuration.

Parameters

value

The maximum allowed number of routes. Range is from 1 through 4294967295.

Modes

VRF address-family IPv4 and IPv6 configuration modes

Examples

To configure the maximum number of allowed routes to 3600 for VRF "myvrf" for an IPv4 address family:

```
device# configure terminal
device(config)# vrf myvrf
device(config-vrf-myvrf)# address-family ipv4 unicast
device(vrf-myvrf-ipv4-unicast)# max-route 3600
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Number of links is 1.

Parameters

num-of-links

The number of links. Valid values range from 1 through 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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# configure terminal
device(config)# protocol lldp
device(conf-lldp)# mode tx
```

To enable only the receive mode:

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# mode rx
```

History

Release version	Command history
17s.1.00	This command was introduced.

monitor session

Enables a Port Mirroring session for monitoring traffic.

Syntax

monitor session *session_number*

no monitor session *session_number*

Parameters

session_number
Specifies a session identification number. Valid values range from 1 through 512.

Modes

Global configuration mode

Usage Guidelines

Enter **no monitor session** to delete the port mirroring session.

Examples

To enable session 22 for monitoring traffic:

```
device# configure terminal
device(config)# monitor session 22
```

History

Release version	Command history
17s.1.00	This command was introduced.

mtu

Configures the size—in bytes—of the maximum transmission unit (MTU) for an Layer 2 packet on a physical or LAG (port-channel) interface bound to one more VLANs.

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.

There are no restrictions on the number of MTU profiles within a broadcast domain. Each port, whether physical or LAG, can have a different MTU value. For physical ports, the MTU is configured on the router port's internal VLAN ID (IVID), which is allocated when the router port is configured. For LAG ports, the Layer 2 MTU is configured on the VLAN to which a virtual Ethernet (VE) interface is bound.

Examples

To configure a nondefault Layer 2 MTU globally:

```
device# configure terminal
device(config)# mtu 2000
```

To revert to the global default:

```
device# configure terminal
device(config)# no mtu
```

To configure a nondefault Layer 2 MTU on an Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# mtu 2000
```

To confirm the running configuration in an example switchport context:

```
device# do show running-config interface ethernet 0/1
interface Ethernet 0/31
 speed 40000
 mtu 2000
 switchport
 switchport mode access
 switchport access vlan 1
 no shutdown
```

To configure a nondefault Layer MTU on a port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)# mtu 2000
```

To confirm the running configuration in an example switchport context:

```
device# do show running-config interface Port-channel 10
interface Port-channel 10
 mtu 2000
 switchport
 switchport mode trunk
 switchport trunk allowed vlan all
 switchport trunk tag native-vlan
```

To revert to the default Layer 2 MTU for the above example:

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)# no mtu
```

History

Release version	Command history
17s.1.01	This command was introduced.

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** }

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

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.

The **no** form of the command restores the defaults.

Examples

The following 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
```

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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.

Enter the **no multiplier** command to return to the default setting.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

Commands N - Q

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

Enabling address exchange for the IPv4 address family is enabled. Enabling address exchange for the IPv6 address family is 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

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 EVPN session with a neighbor with the IP address 10.1.1.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 activate
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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!
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The ASN is not replaced.

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

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.

The **no** form of the command disables this feature.

Examples

The following example replaces the ASN globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 as-override
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

min-rx *receive-time*
Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers.

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 specified peer group and sets the BFD holdover interval 12 for VRF instance “green”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf greeen
device(config-bgp-ipv4u-vrf)# neighbor pg1 bfd
device(config-bgp-ipv4u-vrf)# neighbor pg1 bfd holdover-interval 12
```

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

The **disable** keyword or the **no** form of the command removes all neighbor capability for 4-byte ASNs.

Examples

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The **no** form of the command disables ORF capabilities.

Examples

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

neighbor default-originate

Configures the device to send the default route 0.0.0.0 to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate**

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 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 configures the device to stop sending the default route.

Examples

The following example sends the 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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**

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 (optional). 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

Usage Guidelines

The **no** form of the command disables this feature.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 to disable the AS-path check function.

Examples

The following example enables the outbound AS_PATH check function for the BGP IPv4 unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.1.1.1 enable-peer-as-check
```

The following example enables the outbound AS_PATH check function for the BGP IPv6 unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 enable-peer-as-check
```

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
```

History

Release version	Command history
17s.1.01	This command was introduced.

neighbor encapsulation

Sets the encapsulation type for an IPv4 neighbor, IPv6 neighbor, or a peer group.

Syntax

neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } { **nsh** | **vxlan** }

no neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } { **nsh** | **vxlan** }

Command Default

MPLS encapsulation type.

Parameters

IPV4-address
: Specifies an IPv4 address.

IPV6-address
: Specifies an IPv6 address.

peer-group-name
: Specifies a peer group.

nsh
: Specifies NSH encapsulation.

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 specifies the 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
```

History

Release version	Command history
17s.1.01	This command was introduced.

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**]

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

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

Examples

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Examples

The following 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
```

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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
```

History

Release version	Command history
18s.1.00	This command was introduced.

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**]

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

The **no** form of the command removes the local ASN.

Examples

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Routes received in UPDATE messages are not discarded.

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

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

Examples

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**]

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 1 through 2147483647.

threshold
: Specifies the percentage of the value specified by *num* 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.

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 sets the maximum number of 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
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.

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 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

neighbor next-hop-unchanged

Enables BGP to keep the original next-hop while advertising routes to eBGP neighbors.

Syntax

neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } **next-hop-unchanged**

no neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } **next-hop-unchanged**

Command Default

This functionality is not enabled.

Parameters

IPV4-address
Specifies an IPv4 address.

IPV6-address
Specifies an IPv6 address.

peer-group-name
Specifies a peer group.

Modes

Address-family L2VPN EVPN configuration mode

Usage Guidelines

Use the **no** form of this command to disable this functionality.

Examples

To enable BGHP to keep the original next-hop for IPv4, IPv6, and a peer group:

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 192.168.30.2 next-hop-unchanged
device(config-bgp-evpn)# neighbor 2000:20:1::2 next-hop-unchanged
device(config-bgp-evpn)# neighbor my-peer-group next-hop-unchanged
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
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
Password of up to 63 characters in length that can contain 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 the configured 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 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
IPv4 address of the neighbor.

ipv6-address
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.

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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

neighbor prefix-list

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to IP address and mask length.

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

No prefix-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.

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

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

Examples

The following example applies the prefix list "myprefixlist" to incoming advertisements to 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 prefix-list myprefixlist in
```

The following example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 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 prefix-list myprefixlist out
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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). Valid values range 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)# neighbor 10.11.12.13 remote-as 100
```

History

Release version	Command history
17s.1.00	This command was introduced.

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**

Command Default

Private ASNs are not removed from UPDATE messages sent to the neighbor.

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 BGP4 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* }

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. Range is from 1 through 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

Usage Guidelines

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

neighbor route-reflector-client

Configures a neighbor to be 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
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 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 on a host device to configure a neighbor to be a route-reflector client. Once configured, the host device from which the configuration is made acts as a route-reflector server.

The **no** form of the command disables the feature.

Examples

The following example configures a neighbor to be a route-reflector client.

```
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-reflector-client
```

The following example configures a neighbor to be a route-reflector client for VRF instance "red".

```
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 route-reflector-client
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** [**both** | **extended** | **standard**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **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.

both
Sends both standard and extended attributes.

extended
Sends extended attributes.

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

Usage Guidelines

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

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.

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!
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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

Examples

The following example 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
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

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.

The **no** form of the command disables this feature.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
IPv4 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

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+.

The **no** form of the command disables this feature.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Route suppression is not removed.

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

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **ethernet** *slot* **/** *port* | **loopback** *num*| **ve-interface** *vlan_id* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address* | **ethernet** *slot* **/** *port* | **loopback** *num* | **ve-interface** *vlan_id* }

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
IP address of the update source.

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.

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

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

Examples

The following example configures the device to communicate with a neighbor through the specified IPv4 address and Ethernet interface 0/2.

```
device# configure terminal
device#(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 update-source ethernet 0/2
```

History

Release version	Command history
17s.1.00	This command was introduced.

neighbor weight

Specifies a weight that the device will add to routes that are received from the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight**

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. 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

BGP prefers larger weights over smaller weights.

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

Examples

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The **no** form of the command disables this feature.

Examples

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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 removes the default route as the next hop.

Examples

The following example configures the device to use the default route as the next hop.

```
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 example configures the device to use the default route as the next hop.

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

History

Release version	Command history
17s.1.00	This command was introduced.

next-hop-recursion

Enables BGP recursive next-hop lookups.

Syntax

next-hop-recursion

no next-hop-recursion

Command Default

BGP recursive next-hop lookups are not enabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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.

The **no** form of the command disables BGP recursive next-hop lookups.

Examples

The following example enables recursive next-hop lookups for BGP4.

```
device# configure terminal
device(config)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-recursion
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

npb policy route-map

On a physical or port-channel interface, applies a route map as Network Packet Broker (NPB) policy for all ingress traffic.

Syntax

npb policy route-map *route-map-name*

no npb policy route-map *route-map-name*

Command Default

No route map is applied as NPB policy.

Parameters

route-map-name

Specifies the route map. Values range from 1 through 63 ASCII characters.

Modes

Interface sub-type configuration mode

Usage Guidelines

This command is supported only for NPB. If the system mode is currently default, set it to NPB, using the **system-mode** command.

The **no** form of this command removes a route map previously applied for NPB policy.

Examples

The following example applies a route map to a physical interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# npb policy route-map npb_map1
```

The following example applies a route map to a port-channel.

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)# npb policy route-map npb_map1
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified, with support added for port-channels.

ntp authentication-key

Creates an authentication key to associate with the NTP server, thereby enabling NTP authentication.

Syntax

ntp authentication-key *key-id* {**md5** *md5-string* | **sha1** *sha1-string*}**encryption-level** *enc_value*

no ntp authentication-key *key-id*

Command Default

NTP authentication is disabled by default.

Parameters

key-id
Specifies an ID for an authentication key. The range is from 1 through 65535.

md5 *md5-string*
Specifies a string for the MD5 message-digest algorithm. The string can be a maximum of 15 ASCII characters.

encryption-level *enc_value*
Defines the level of encryption for the NTP authentication key. The valid values are 0 and 7. The value 0 is clear text format and the value 7 is fully encrypted format. The default value is 7.

sha1 *sha1-string*
Specifies a string for SHA1 encryption. 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ntp server

Specifies or adds an NTP server IP address and optionally associates an authentication key to the server.

Syntax

ntp server *ip-address* [**key** *key-id*] [**use-vrf** *vrf-name*]

no ntp server *ip-address* [**key** *key-id*] [**use-vrf** *vrf-name*]

Command Default

The NTP server list is LOCL (no NTP server configured).

Parameters

ip-address
: Specifies the NTP server IPv4 IP address (dot-decimal notation) or the IPv6 IP address (hexadecimal colon-separated notation).

key *key-id*
: Associates a key from the key list to the specified server. The range for a key ID is from 1 through 65535.

use-vrf *vrf-name*
: Specifies a VRF through which to communicate with the NTP server. See the Usage Guidelines.

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

To associate a configured key ID of 15 to an NTP server on the management VRF:

```
device# configure terminal
device(config)# ntp server 192.168.10.1 key 15
```

To associate a configured key ID of 15 to an NTP server on a user-specified VRF:

```
device# configure terminal
device(config)# ntp server 192.168.10.1 key 15 use-vrf myvrf
```

To remove an NTP server from the current list of NTP servers on the management VRF:

```
device# configure terminal
device(config)# no ntp server 192.168.10.1
```

History

Release version	Command history
17s.1.00	This command was introduced.

ntp source-ip

Configures the source IP address to be used to access the NTP server.

Syntax

ntp source-ip chassis-ip *ip_address*

no ntp source-ip

Command Default

The NTP source IP is not configured.

Parameters

chassis-ip *ip_address*
Uses the IP address of the chassis for the NTP server.

Modes

Global configuration mode

Usage Guidelines

Use the **no ntp source-ip** command to remove the configuration.

Examples

Typical command example:

```
device# configure terminal
device(config)# ntp source-ip chassis-ip 10.28.52.26
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 Extreme 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
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This topic was modified to reflect the modification of the **start-shell** command. Even after entering **start-shell**, you cannot access Linux commands that require root permissions.

overlay-class-map

Specifies an overlay class map and enters overlay-class-map configuration mode

Syntax

overlay-class-map *class-map-name*

no overlay-class-map *class-map-name*

Command Default

No overlay class map is created.

Parameters

class-map-name

Name of an overlay class map. The map name is restricted to 63 characters. See the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

Enter **no overlay-class-map***class-map-name* while in global configuration mode to remove the overlay class map.

The following rules govern overlay policy maps:

- An overlay policy map name must begin with a–z, A–Z or 0–9. Underscore and hyphen can also be used, except as the first character, and the name length can not exceed 63 characters.
- The overlay policy must contain an overlay-class-map directive that contains the information necessary to identify the tunnel or tunnels on which the policy is to apply.
- The overlay policy must contain at least one statement for matching the inner flow (achieved through ACL matching) and the action to take on the matching flow. The supported actions are any existing ACL security action (permit or deny), as well as any desired flow-based QoS result (for example, sampling or mirroring).
- Forward referencing of ACLs or service-policy maps is not allowed. The user must first define the objects to be contained in the policy map (ACLs or Qos service maps) before referencing them in an overlay policy map. The forward referencing of an object causes an error to be returned during such a configuration.

Examples

The following creates an overlay class map and place the system into overlay classmap configuration mode.

```
device# configure terminal
device(config)# overlay-class-map overlayclassmap1
device(config-overlay-classmap-overlayclassmap1)#
```

Once the map is created, criteria must be matched by means of the **seq** command, as in the following example.

```
device(config-overlay-classmap-overlayclassmap1)# seq 0 match source 1.1.1.1 encap-type vxlan vni 50
```

The following example removes the overlay class map.

```
device# configure terminal
device(config)# no overlay-class-map overlayclassmap1
```

History

Release version	Command history
17s.1.01	This command was introduced.

overlay-gateway

Creates a VXLAN overlay gateway instance and enables VXLAN overlay gateway configuration mode.

Syntax

overlay-gateway *name*

no overlay-gateway *name*

Command Default

The default VXLAN overlay gateway setting for **type** is **layer2-extension**.

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. The objectives of setting up a gateway are:

- Configuring the source IP address
- Configuring the VLAN or VLANs
- 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 4 Key commands available in VXLAN overlay gateway configuration mode

Command	Description
activate	Activates a VXLAN overlay gateway instance.
attach vlan	Specifies exported VLANs or MAC addresses in VXLAN overlay gateway configurations
describe	Describes the overlay gateway.
ip interface	Sets the IP address of a VXLAN overlay gateway instance.
map vlan vni	In a VXLAN overlay gateway configuration that uses Layer 2 extension, associates VLANs with VXLAN Network Identifiers (VNIs).

TABLE 4 Key commands available in VXLAN overlay gateway configuration mode (continued)

Command	Description
site	Configures a remote Layer 2 extension site in a VXLAN overlay gateway context.
type	Specifies whether a VXLAN overlay gateway uses NSX Controller integration or Layer 2 extension.

Only one VXLAN overlay gateway instance can be configured per system.

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, and then enter the **activate** command.

Examples

The following example creates a VXLAN overlay gateway instance named "gateway1" and enter VXLAN overlay gateway configuration mode.

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

History

Release version	Command history
17s.1.01	This command was introduced.

overlay-policy-map

Configures an overlay policy map containing a class map so that you can apply policer and QoS attributes to a particular interface.

Syntax

overlay-policy-map *policy-mapname*

no overlay-policy-map *policy-mapname*

Command Default

No overlay policy map is created.

Parameters

policy-mapname
Name of an overlay policy map.

Modes

Global configuration mode

Usage Guidelines

When you execute the **overlay-policy-map** command, the system is placed in config-overlay-policy-map configuration 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. The class map can be associated with specific policing and QoS parameters.

Associate the policy map to the interface for the inbound direction by means of the **overlay-service-policy** command.

Enter **no overlay-policy-map** *policy-mapname* while in global configuration mode to remove the policy map.

Examples

The following example creates an overlay policy map and places the system into overlay policymap configuration mode so that you can add a class map.

```
device# configure terminal
device(config)# overlay-policy-map overlaypolicymap1
device(config-overlay-policymap)#
```

Once the map is created, you must attach the overlay policy map and QoS actions, security ACLs, or both, by means of the **seq** and **ip access-group** commands, as in the following example.

```
device(config)# overlay-policy-map overlaypolicymap1
(config-overlay-policymap-overlaypolicymap1)# seq 10 overlay-class tunnel-group-1
device(config-overlay-policymap-class-tunnel-group-1)# ip access-group test
device(config-overlay-policymap-class-tunnel-group-1)# exit
device(config-overlay-policymap-overlaypolicymap1)# exit
```

The following example removes the policy map.

```
device# configure terminal
device(config)# no overlay-policy-map overlaypolicymap1
```

History

Release version	Command history
17s.1.01	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.01	This command was introduced.

overlay-transit

Creates a VXLAN overlay transit instance.

Syntax

overlay-trnasit *name*

no overlay-transit *name*

Command Default

This feature is not enables.

Parameters

name

Specifies a name for the VXLAN overlay transit instance. 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 transit instance on a spine node. From there the **overlay-service-policy** command is available, through which the user can enter VXLAN overlay service policy configuration mode.

Examples

The following example creates a VXLAN overlay transit instance named "myOTinstance" and enables VXLAN overlay gateway configuration mode.

```
device# configure terminal
device(config)# overlay-transit myOTinstance
device(config-overlay-transit-myOTinstance)#
```

History

Release version	Command history
17s.1.01	This command was introduced.

owner

Allows owner preemption and tracked interface priority configuration for a virtual router designated as the Virtual Router Redundancy Protocol (VRRP) owner.

Syntax

owner priority *value*

owner track-priority *value*

no owner priority *value*

no owner track-priority *value*

Command Default

The VRRP owner priority is set to 255 and interface tracking priorities are set individually.

Parameters

priority *value*
: Enables owner preemption by setting the priority of the VRRP owner device to be less than the default value. Value can be from 1 to 254.

track-priority *value*
: Sets the owner track priority value if the tracked port fails. The tracked interface value configured for the owner device overrides any configured individual tracked interface priorities. Value can be from 1 to 254. Default is 2.

Modes

Virtual-router-group configuration mode

Usage Guidelines

VRRP owner preemption allows a lower device priority to be set and if a backup VRRP device has a higher priority, the backup device assumes the master VRRP role and the current owner device becomes a backup device. If an owner track priority is configured, the backup device priority must be higher than the combination of the owner priority and the current tracked interface priorities.

The **no owner priority** command disables owner preemption and reverts the priority value to 255.

The **no owner track-priority** command removes the owner track priority, allowing individual interface track priorities to be used.

Examples

The following example configures the VRRP owner device priority to 200 and the tracked interface priority to 20.

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 0/6
device(conf-if-eth-0/6)# ip address 192.168.4.1/24
device(conf-if-eth-0/6)# vrrp-group 1
device(config-vrrp-group-1)# virtual-ip 192.168.4.1
device(config-vrrp-group-1)# owner priority 200
device(config-vrrp-group-1)# owner track-priority 20
```

History

Release version	Command history
17s.1.00	This command was introduced.

password-attributes

Configures global password attributes.

Syntax

password-attributes { [**max-retry** *maxretry*] [**min-length** *minlen*] [**max-lockout-duration** *duration*] [**admin-lockout** | **character-restriction** { [**lower** *numlower*] [**numeric** *numdigits*] [**special-char** *numsplchars*] [**upper** *numupper*] } }

no password-attributes { [**max-retry** *maxretry*] [**min-length** *minlen*] [**max-lockout-duration** *duration*] [**admin-lockout** | **character-restriction** { [**lower** *numlower*] [**numeric** *numdigits*] [**special-char** *numsplchars*] [**upper** *numupper*] }] }

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, nonalphanumeric 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-retry *maxretry*

Specifies 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 *minlen*

Specifies the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

max-lockout-duration *duration*

Specifies the maximum number of minutes after which the user account is unlocked. Range is from 0 through 99999. The default is 0, representing an infinite duration.

Modes

Global configuration mode

Usage Guidelines

To reset password attributes to their default values, enter the **no** form of this command.

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 specifies that the user account be unlocked after 5 minutes and enables lockout policy for admin role accounts.

```
device#configure terminal
device(config)# password-attributes max-lockout-duration 5 admin-lockout
```

History

Release version	Command history
17s.1.00	This command was introduced.

pbf destination

Creates a policy-based forwarding (PBF) destination and accesses PBF-destination configuration mode.

Syntax

pbf destination *pbf-destination-id*

no pbf destination *pbf-destination-id*

Command Default

No PBF destinations are defined.

Parameters

pbf-destination-id

Specifies a policy-based forwarding (PBF) destination. ID values range from 1 through 8192.

Modes

Global configuration mode

Usage Guidelines

The use-case for this command is under Network Packet Broker (NPB) system mode.

The PBF-destination ID must be unique across all devices managed on the Extreme Visibility Manager instance.

Use the **no** form of this command to delete a PBF destination.

Examples

The following example defines a PBF destination and accesses PBF-destination configuration mode.

```
device# configure terminal
device(config)# pbf destination 20
device(config-destination-20)# precedence 10 set interface port-channel 5
device(config-destination-20)# precedence 30 set interface ethernet 0/3
device(config-destination-20)# statistics-enable
```

History

Release version	Command history
18s.1.02	This command was introduced.

pbf destination-group

Creates a policy-based forwarding (PBF) destination-group and accesses PBF destination-group configuration mode.

Syntax

pbf destination-group *pbf-dest-group-id*

no pbf destination-group *pbf-dest-group-id*

Command Default

No PBF destination-groups are defined.

Parameters

pbf-dest-group-id

Specifies a policy-based forwarding (PBF)-destination group. Values range from 1 through 8192.

Modes

Global configuration mode

Usage Guidelines

The use-case for this command is under Network Packet Broker (NPB) system mode.

Use the **no** form of this command to delete a PBF destination-group.

Examples

The following example creates or accesses a PBF distribution group and adds destinations to it.

```
device# configure terminal
device(config)# pbf destination-group 100
device(config-destination-group-100)# add destination 10,20,30
```

History

Release version	Command history
18s.1.02	This command was introduced.

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 peer IP address is the remote MCT node IP address.

Modes

Cluster configuration mode.

Usage Guidelines

Configure a corresponding neighbor in BGP EVPN address family for the peer. If the peer is already configured as a neighbor, when you deploy and undeploy the cluster, the BGP neighbor resets to renegotiate its capability.

If the peer already exists for other address family, clear the IP BGP peer session.

The **no** form of the command deletes the peer IP address configuration.

The **no peer** command causes a controlled failover and the target node is removed permanently from the cluster. Primary and secondary controlled failover is supported, as is primary and secondary uncontrolled failover (on loss of heartbeat).

If, for example, Node A is aware of its peer, Node B, and Node B is not aware of Node A, then Node A becomes the principal node. This can happen if the **no peer** command is executed on only a single node in the cluster.

You cannot change the peer when the cluster is deployed.

Examples

The following example shows the configuring of the cluster peer IP address.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# peer 10.10.10.12
```

History

Release version	Command history
17s.1.01	This command was introduced.
17s.1.02	Added usage guidelines for the **no peer** command.

peer-interface

Configures the Ethernet or port channel interface to reach the MCT cluster peer.

Syntax

peer-interface Ethernet 0/*port* | **port-channel** *ID*

no peer-interface

Parameters

Ethernet 0/*port*

Specifies the Ethernet port for the cluster peer.

port-channel *ID*

Specifies the port channel interface for the cluster peer.

Modes

Cluster configuration mode.

Usage Guidelines

The **no** form of the command deletes the peer interface configuration.

The peer interface must be a Layer 2 interface. When it is configured, it is an internal switch port.

An external switch port or Layer 3 configuration is not allowed on a peer interface.

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# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# peer-interface port-channel 10
```

History

Release version	Command history
17s.1.01	This command was introduced.

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.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*]] [**classification-type** *classification-type-name*] [**remark-profile** *profile-name*]

no police { **cir** [**cbs**] [**eir** [**ebs**]] [**classification-type**] [**remark-profile**] }

Parameters

cir-bps
Specifies the committed information rate in bits per second. Enter an integer from 18000 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.

classification-type *classification-type-name*
Specifies the name of the classification type for remarking. Choices include the following:

- color-and-cos
- color-and-dscp
- color-and-traffic-class

remark-profile *profile-name*
Specifies the remark profile that contains the parameters used for remarking.

Modes

Policy-map class configuration mode

Usage Guidelines

Use the **no** version of this command to remove the parameter from the class map.

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 parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

police-remark-profile

Allows you to modify the default profile used for policer remarking. Only the default profile is supported.

Syntax

police-remark-profile *profile-name*

Command Default

The existing settings in the default profile.

Parameters

profile-name

The name of the profile. For policing remarking, only **default** is supported.

Modes

Global configuration mode

Usage Guidelines

You can edit the default profile, but you cannot delete it. The attributes in the default remark profile are those that were specified during the latest modification. If the remark profile has never been modified, then the options are those that were specified in the default remark profile provided during initialization.

After you execute the **police-remark-profile** command, you use the **action**, **set**, and **map** commands to modify the settings in the policer remark profile.

Examples

The following is an example of executing the **police-remark-profile** command to begin the process of modifying the default policer remark profile. The example also shows using the **action** command to specify the color classification type for conforming traffic. Then, the example shows using the **set** command to specify the settings for the remark values in the default policer remark profile.

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color conform
device(police-remark-profile-color-conform)# set cos 3
device(police-remark-profile-color-conform)# set traffic-class 5
device(police-remark-profile-color-conform)# set dscp 10
device(police-remark-profile-color-conform)# exit
```

The following is an example of executing the **police-remark-profile** command to begin the process of modifying the default policer remark profile. The example also shows using the **action** command to specify the color-and-cos classification type for exceed traffic. Then, the example shows using the **map** command to specify the maps to be included in the default policer remark profile for cos remarking for exceeding traffic. ("cm1," "ct1," and "cd1" are map names).

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color-and-cos exceed
device(police-remark-profile-color-and-cos-exceed)# map cos-mutation cm1
device(police-remark-profile-color-and-cos-exceed)# map cos-traffic-class ct1
device(police-remark-profile-color-and-cos-exceed)# map cos-dscp cd1
device(police-remark-profile-color-and-cos-exceed)# exit
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The class map can be associated with specific policing and QoS parameters.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

port

Defines the TCP connection port of the LDAP host.

Syntax

port { *portnum* }

no port

Command Default

The default port is 389.

Parameters

portnum

Specifies the TCP port used to connect the AD server for authentication. The port range is from 1 through 65535.

Modes

LDAP host configuration mode.

Usage Guidelines

Use the no form of this command to remove the port.

Examples

To add an LDAP server on port 3890:

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# port 3890
```

Executing **no** on an attribute sets it with its default value.

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# no port
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

priority1

In PTP configuration mode, specifies a nondefault clock Priority1 value for selecting the Precision Time Protocol best master clock (BMC).

Syntax

priority1 *priority*

no priority1

Command Default

See the Usage Guidelines.

Parameters

priority

The clock Priority1 value used by the Best Master Clock Algorithm (BMCA). Range is from 0 through 255. The default is 255. See the Usage Guidelines.

Modes

PTP configuration mode

Usage Guidelines

The value for this setting influences whether the node can be elected a grandmaster (GM) clock or not. In practical deployments, the default value (255) is recommended. The GM clock, if present, takes over.

Use the **no** form of this command to revert to the default Priority1 value.

Examples

To change the value of the BMCA Priority1 field from the default:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# priority1 10
```

To revert to the default Priority1 value:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# no priority1
```

History

Release version	Command history
17s.1.00	This command was introduced.

priority2

In PTP configuration mode, specifies a nondefault clock Priority2 value for selecting the Precision Time Protocol best master clock (BMC).

Syntax

priority2 *priority*

no priority2

Command Default

See the Usage Guidelines.

Parameters

priority

The clock Priority2 value used by the Best Master Clock Algorithm (BMCA). Range is from 0 through 255. The default is 255.

Modes

PTP configuration mode

Usage Guidelines

The Priority2 value is used by the BMCA to decide between two devices that are otherwise equally matched with respect to default selection criteria (such as clock quality, clock class, and clock stability).

Use the **no** form of this command to revert to the default Priority2 value.

Examples

To change the value of the BMCA Priority2 field from the default:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# priority2 20
```

To revert to the default Priority2 value:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# no priority2
```

History

Release version	Command history
17s.1.00	This command was introduced.

priority-group-table

Configures the CEE priority group table mapping for the Priority Group ID (PGID).

Syntax

priority-group-table *pgid* **weight** *weight* **pfc** { **on** | **off** }

no priority-group-table *pgid*

Command Default

See the following table for the default settings for each PGID.

PGID	Bandwidth% (DWRR weight)	Priority flow control (PFC)
15.0	-	N
15.1	-	N
15.2	-	N
15.3	-	N
15.4	-	N
15.5	-	N
15.6	-	N
15.7	-	N
0	0	N
1	40	Y
2	60	N
3	0	N
4	0	N
5	0	N
6	0	N
7	0	N

Parameters

pgid

Specifies the PGID.

weight *weight*

Specifies the DWRR weight which is the percentage of bandwidth. Enter an integer from 1 to 100.

pfc

Specifies the priority flow control setting.

off

Disables priority flow control.

on

Enables priority flow control.

Modes

CEE map configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default settings for the specified PGID.

When any of the PGID 0 through 7 is activated, a bandwidth percentage must be specified. The bandwidth percentage is the percentage of the link bandwidth that the Priority Group should receive during periods of link oversubscription after all Strict Priority Group have been serviced and is used to derive DWRR weight.

Relative priority between Priority Groups is exactly the ordering of entries listed in the table in the Command Default, with PGID 15.0 being highest priority and PGID 15.7 being lowest priority.

Congestion control configuration is partially specified by enabling or disabling PFC because the set of priorities mapped to the Priority Group is not known. The CEE Priority Table configuration through the **priority-table** command completes the PFC configuration.

Examples

The following example configures PGID 0.

```
device# configure terminal
device(config)# cee-map default
device(config-cee-map-default)# priority-group-table 0 weight 50 pfc on
```

History

Release version	Command history
17s.1.00	This command was introduced.

priority-table

Maps the priority (CoS) to the CEE priority group.

Syntax

priority-table *PGID_CoS0 PGID_CoS1 PGID_CoS2 PGID_CoS3 PGID_CoS4 PGID_CoS5 PGID_CoS6 PGID_CoS7*

no priority-table

Command Default

The mapping of all CoS priorities is to priority group (PGID) 2.

Parameters

PGID_CoS0
Specifies the PGID that maps to COS 0.

PGID_CoS1
Specifies the PGID that maps to COS 1.

PGID_CoS2
Specifies the PGID that maps to COS 2.

PGID_CoS3
Specifies the PGID that maps to COS 3.

PGID_CoS4
Specifies the PGID that maps to COS 4.

PGID_CoS5
Specifies the PGID that maps to COS 5.

PGID_CoS6
Specifies the PGID that maps to COS 6.

PGID_CoS7
Specifies the PGID that maps to COS 7.

Modes

CEE-map configuration mode

Usage Guidelines

Use the no form to reset the default setting of PGID 2.

The PFC configuration is completed when the CEE Priority Table defining which CoS maps to a PGID is combined with the CEE Priority Group Table configuration indicating whether PFC is enabled or disabled for the Priority Group.

Examples

The following example configures the priority-table map.

```
device# configure terminal
device(config)# cee-map default
device(config-cee-map-default)# priority-table 1 1 1 0 1 1 1 15.0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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. SLX 9240 supports 128 active profiles and SLX 9140 supports 72 active profiles.

Enter the **no profile** *name* command 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 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 event-profile default_event_statistics

no profile event-profile default_event_statistics

profile interface-profile default_interface_statistics

no profile interface-profile default_interface_statistics

profile lldp default_lldp_statistics

no profile lldp default_lldp_statistics

profile pbr default_pbr_statistics

no profile pbr default_pbr_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
Specifies profile **default_enhanced_queue_discard_pkts_statistics** of the **enhanced-queue-discard-pkts-profile** profile type—for tracking discarded-packet statistics.

event-profile default_event_statistics
Specifies profile **default_event_statistics** of the **event** profile type—for tracking event statistics.

interface-profile default_interface_statistics
Specifies profile **default_interface_statistics** of the **interface-profile** profile type—for tracking interface statistics.

lldp-profile default_lldp_statistics
Specifies profile **default_lldp_statistics** of the **lldp** profile type—for tracking LLDP statistics.

pbr default_pbr_statistics
Specifies profile **default_lldp_statistics** of the **pbr** profile type—for tracking policy-based routing (PBR) statistics.

queue-profile default_queue_statistics
Specifies profile **default_queue_statistics** of the **queue-profile** profile type—for tracking queue statistics.

system-profile default_system_utilization_statistics

Specifies profile **default_system_utilization_statistics** of the **system-profile** profile type—for tracking system utilization statistics.

Modes

Telemetry-collector configuration mode

Usage Guidelines

You can apply multiple telemetry profiles to a collector.

The **no** version of the command removes a telemetry profile from a collector.

Examples

The following example assigns two profiles to a collector.

```
device# configure terminal
device(config)# telemetry collector collector_1
device(config-collector-collector_1)# profile system-utilization default_system_utilization_statistics
device(config-collector-collector_1)# profile interface-profile default_interface_statistics
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.00	Added support for **enhanced-queue-discard-pkts-profile** and **queue-profile** profile types.
18s.1.02	Added support for **event-profile**, **lldp-profile**, and **pbr-profile** profile types.

profile ipv6-lookup

Specifies the IPv6 address lookup-mode.

Syntax

profile ipv6-lookup { **default** | **network-id** }

Command Default

The default IPv6 address lookup mode is by host ID.

Parameters

default

Resets the IPv6 address lookup-mode to host ID (bits 64–127 of the IPv6 address).

network-id

Changes the IPv6 address lookup-mode to network ID (bits 0–63 of the IPv6 address).

Modes

Hardware configuration mode

Usage Guidelines

ATTENTION
This is a disruptive command. In order for the last update of the profile configuration to take effect on a device, you must run the **copy running-config startup-config** command followed by the **reload system** command.

This command is available only in network packet broker (NBP) system-mode.

Each forwarded frame has a token with a 100-byte header buffer for storing header data. Fields copied into this token header-buffer are available for lookup (to make forwarding decisions). Because of this small buffer size, copying the entire 128-bit SIP and DIP addresses is not supported. You can configure the IPv6 lookup profile, specifying which half of SIP and DIP addresses are copied into the buffer:

- (Default) Host ID (bits 64-127)
- Network ID (bits 0-63)

The software does not prevent you from specifying a full 128-bit IPV6 address while configuring an IPv6 ACL. However, only the half configured in the IPv6 lookup profile is matched.

Before you change lookup-profile, you need to evaluate the impact of the change on current IPv6 ACLs.

There is not a **no** form of this command.

Examples

The following example changes the IPv6 lookup-profile from the default host-ID (bits 64-127) mode to network-id (bits 0-63) mode.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile ipv6-lookup network-id
%Warning: To activate the new profile config, please run 'copy running-config startup-config' followed
by 'reload system'.
```

The following example restores the default IPv6 host-ID lookup-profile.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile ipv6-lookup default
%Warning: To activate the new profile config, please run 'copy running-config startup-config' followed
by 'reload system'.
```

History

Release version	Command history
18s.1.00	This command was introduced.

profile overlay-visibility

Configures hardware profile settings related to overlay visibility.

Syntax

profile overlay-visibility { **default** | **endpoint** | **endpoint-vni**| **tunnel-vni**| **vni**}

Command Default

Default hardware profile settings are configured.

Parameters

default
Configures a match on outer source IP and destination IP addresses.

endpoint
Configures a match on outer source IP or destination IP addresses.

endpoint-vni
Configures a match on outer source IP address and virtual network identifier (VNI), or destination IP address and VNI.

tunnel-vni
Configures a match on outer source IP address, destination IP address, and VNI.

vni
Configures a match on VNI only.

Modes

Hardware configuration mode

Usage Guidelines

The overlay visibility profile must be set to the appropriate classification method. If the class map rules do not match the visibility profile that is selected, the classification is not programmed into the hardware when applied within the context of an overlay transit service.

Use the **show hardware profile overlay-visibility** command, with the keywords as shown above, to confirm the settings of the **profile overlay-visibility** command.

Examples

The following example sets the overlay visibility profile to match on the VNI only.

```
device# configure terminal
device(config)# hardware
device(config-hardware)$ profile overlay-visibility vni
```

History

Release version	Command history
17s.1.01	This command was introduced.

profile route-table

Optimizes hardware forwarding resources for route tables.

Syntax

profile route-table { **default** | **ipv4-max-arp** | **ipv6-max-nd** | **multicast** | **multicast-snoop** | **user-defined** } [**maximum_paths** { **8** | **16** | **32** | **64** }]

Command Default

The default hardware profiles are enabled.

Parameters

default
Optimizes IPv4/IPv6 resources for dual-stack operations.

ipv4-max-arp
Optimizes resources for IPv4 unicast with maximum ARP.

ipv6-max-nd
Optimizes resources for IP unicast and IPV6 routing with maximum ND.

multicast
Optimizes resources for IP unicast dual stack and IPv4 mulitcast.

multicast-snoop
Optimizes resources for IP unicast dual stack and multicast snooping.

user-defined
Optimizes resources for the user-defined profile.

maximum_paths
Specifies 8, 16, 32, or 64 as the maximum number of load-sharing paths.

Modes

Hardware configuration mode

Usage Guidelines

ATTENTION
This is a disruptive command. In order for the last update of the profile configuration to take effect on a device, you must run the **copy running-config startup-config** command followed by the **reload system** command.

This configuration command configures the route-table hardware forwarding resource allocation to optimize the specified protocol functionality.

The maximum-path variable is optional. If skipped, the maximum-path remains unchanged. This parameter is not supported for the user-defined subtype.

There is not a **no** form of this command.

The detailed layout of user-defined profile is not configured through the CLI interface. Instead, you must lay out the profile details in an .xml file that will be pre-loaded onto the switch to a pre-defined location and consumed by platform/ASIC modules as the device boots up.

The device boots up in pre-defined default hardware profile and with no user-defined profile. The default version of user-defined profile that comes with the release package is present on the device. Follow the suggested procedure to create and deploy user-defined profile. You can use it as a template to compile your own based on your needs.

Use the **copy user-defined-profile file-url** command to upload your version of the user-defined profile to the device. The default user-defined profile that comes with the release package is always available.

The locations for user-defined profile and the default template from the release package are:

- /var/config/profile/user-defined
- /var/config/profile/default-profile

As the device boots up, if the hardware profile is specified to be user-defined, then the software loads the profile from this location to initialize ASIC resource allocation.

Examples

To optimize route profiles with a maximum of 16 paths for IIPv4 unicast with maximum ARP:

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile route-table ipv4-max-arp maximum_paths 16
```

History

Release version	Command history
17s.1.00	This command was introduced.

profile tcam

Optimizes hardware resources for ternary content-addressable memory (TCAM) profiles.

Syntax

profile tcam{ **default** | **l2-l3iacl** | **l2-l3iqos**| **l3-acl** |**l3-iacl-l2-eacl** | **l3-iacl-l2-iqos** |**l3-iqos-l2-iacl** | **user-defined** }

profile tcam{ **default** | **l2-acl-l3-iacl** | **l2-iacl-l3-acl**| **l2-l3-iacl-l2-iqos** |**l2-l3-iqos-l2-iacl** | **l2-l3-iqos-l3-iacl** |**l2-l3-iqos-l2-eacl** |**l2-l3-iqos-l3-eacl** | **user-defined** }

profile tcam{ **default** | **app-tele-l3-iqos-l2-iacl**| **app-tele-l3-iqos-l3-iacl** | **user-defined**}

Command Default

The default hardware profiles are enabled.

Parameters

default
Optimizes resources with basic support for all applications.

l2-l3iacl
Optimizes resources for ingress L2 and ingress IPv4, and IPv6 ACLs. Valid for the SLX 9240.

l2-l3iqos
Optimizes resources for ingress L2, IPv4, and IPv6 QoS. Valid for the SLX 9240.

l3-acl
Optimizes resources for ingress, egress IPv4, and IPv6 ACLs. Valid for the SLX 9240.

l3-iacl-l2-eacl
Optimizes resources for ingress IPv4, IPv6 ACL, and egress L2 ACLs. Valid for the SLX 9240.

l3-iacl-l2-iqos
Optimizes resources for ingress IPv4, IPv6 ACL, and ingress L2 QoS. Valid for the SLX 9240.

l3-iqos-l2-iacl
Optimizes resources for ingress IPv4, IPv6 Qos, and ingress L2 ACLs. Valid for the SLX 9240.

default
Optimizes resources with basic support for all applications.

l2-acl-l3-iacl
Optimizes resources for ingress, egress L2 ACL & ingress IPv4, IPv6 ACL. Valid for the SLX 9140.

l2-iacl-l3-acl
Optimizes resources for ingress L2 ACL & ingress, egress IPv4, IPv6 ACL. Valid for the SLX 9140.

l2-l3-iacl-l2-iqos
Optimizes resources for ingress L2, IPv4, IPv6 ACL & ingress L2 QoS. Valid for the SLX 9140.

l2-l3-iqos-l2-iacl
Optimizes resources for ingress L2, IPv4, IPv6 Qos & ingress L2 ACL. Valid for the SLX 9140.

l2-l3-iqos-l3-iacl
Optimizes resources for ingress L2, IPv4, IPv6 Qos & ingress IPv4, IPv6 ACL. Valid for the SLX 9140.

l2-l3-iqos-l2-eacl
Optimizes resources for ingress L2, IPv4, IPv6 Qos & egress L2 ACL. Valid for the SLX 9140.

l2-l3-iqos-l3-eacl
Optimizes resources for ingress L2, IPv4, IPv6 Qos & egress IPv4, IPv6 ACL. Valid for the SLX 9140.

app-tele-l3-iqos-l2-iacl
Optimizes resources for ingress application telemetry, IPv4, IPv6 QOS & L2 ACL. Valid for the SLX 9140.

app-tele-l3-iqos-l3-iacl
Optimizes resources for ingress application telemetry, IPv4, IPv6 QOS & IPv4, IPv6 ACL. Valid for the SLX 9140. The profile is as follows.

user-defined
Optimizes resources for user-defined profiles.

Modes

Hardware configuration mode

Usage Guidelines

ATTENTION
This is a disruptive command. In order for the last update of the profile configuration to take effect on a device, you must run the **copy running-config startup-config** command followed by the **reload system** command.

There is not a **no** form of this command.

The detailed layout of user-defined profile is not configured through the CLI interface. Instead, you must lay out the profile details in an .xml file that will be pre-loaded onto the switch to a pre-defined location and consumed by platform/ASIC modules as the device boots up.

The device boots up in pre-defined default hardware profile and with no user-defined profile. The default version of user-defined profile that comes with the release package is present on the device. Follow the suggested procedure to create and deploy user-defined profile. You can use it as a template to compile your own based on your needs.

Use the **copy user-defined-profile file-url** command to upload your version of the user-defined profile to the device. The default user-defined profile that comes with the release package is always available.

The locations for user-defined profile and the default template from the release package are:

- /var/config/profile/user-defined
- /var/config/profile/default-profile

As the device boots up, if the hardware profile is specified to be user-defined, then the software loads the profile from this location to initialize ASIC resource allocation.

Examples

To optimize TCAM resources for multicast:

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile tcam l2-l3iacl
```

To optimize TCAM resources for Application Telemetry enables the profile to support IPv4, IPv6 QoS, and Layer 2 ACLs:

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile tcam app-tele-l3-iqos-l2-iacl
```

Release version	Command history
17s.1.00	This command was introduced.
18s.1.01	This command was modified to support application telemetry.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

protocol ptp

Enters Precision Time Protocol (PTP) configuration mode.

Syntax

protocol ptp

no protocol ptp

Command Default

PTP is disabled.

Modes

Global configuration mode

Interface subtype configuration mode

Usage Guidelines

In PTP configuration mode, the user can enable or disable PTP, specify clock-quality parameters used by the the Best Master Clock Algorithm (BMCA), and specify the transmission frequency of messages used to update the PTP clock.

This command is not allowed on interfaces that are part of a port channel.

The **no** form of this command at the switch (global) level deletes PTP configurations and reverts to the default (factory shipped) configuration. Interface-level configurations are not affected.

The **no** form of this command at the interface level removes PTP configurations from the interface.

Examples

To enter PTP configuration mode at the switch level:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)#
```

To enter PTP configuration mode at the interface level:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# protocol ptp
device(conf-if-eth-0/1)#
```

To disable PTP at the switch level and set all parameters previously entered under this mode to the default:

```
device# configure terminal
device(config)# no protocol ptp
device(config)#
```

To disable PTP configuration mode at the interface level and set all parameters previously entered under this mode to the default:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no protocol ptp
device(conf-if-eth-0/1)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ptp-vlan

Configures the VLAN used to transmit Precision Time Protocol (PTP) frames on a switch port.

Syntax

ptp-vlan *vlan-id*

no ptp-vlan

Command Default

See the Usage Guidelines.

Parameters

vlan-id

A valid VLAN ID.

Modes

PTP configuration mode

Interface subtype configuration mode

Usage Guidelines

If a VLAN is not specified, the default VLAN is the access VLAN on an access port, and the native VLAN on a trunk port.

If the VLAN specified is not one of the configured VLANs on the switch port, PTP frames are not sent.

If the STP state for the specified VLAN is blocked, PTP frames are not sent.

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

Examples

To configure PTP VLAN 100 on a trunk port:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# switchport trunk allow vlan add 100-200
device(conf-if-eth-0/1)# protocol ptp
device(conf-if-eth-0/1-ptp)# enable
device(conf-if-eth-0/1-ptp)# ptp-vlan 100
```

To remove the PTP VLAN:

```
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 ptp-vlan
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 convention is to use lower-case.
- Python syntax is case sensitive.

To exit the Python environment and return to the SLX-OS 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 3.3.2 (default, Apr 11 2014, 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* under "Python Event-Management and Scripting" and "Python scripts and run-logs."

```
device# python create_po.py
!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan dot1q tag native

!Command: config
 vlan 101-105
!Time: Mon Aug 22 18:33:03 2016

!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan 101
!
vlan 102
!
vlan 103
!
vlan 104
!
vlan 105
!
vlan dot1q tag native

!Command: show running-config int po
!Time: Mon Aug 22 18:33:03 2016

interface Port-channel 1
 description Insight port-channel on MM1
 shutdown
!
interface Port-channel 2
 description Insight port-channel on MM2
 shutdown
!
!Command: config
 int po 10
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 101-105
 switchport trunk tag native-vlan ; no shut
!Time: Mon Aug 22 18:33:03 2016


!Command: show running-config int po
!Time: Mon Aug 22 18:33:04 2016

interface Port-channel 1
 description Insight port-channel on MM1
 shutdown
!
interface Port-channel 2
 description Insight port-channel on MM2
 shutdown
!
interface Port-channel 10
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 101-105
```

```
 switchport trunk tag native-vlan
 no shutdown
!

!Command: config
 int eth 0/4
 channel-group 10 mode active type standard
 no shut
!Time: Mon Aug 22 18:33:04 2016


!Command: show running-config int eth 0/4
!Time: Mon Aug 22 18:33:04 2016

interface Ethernet 0/4
 channel-group 10 mode active type standard
 lacp timeout long
 no shutdown
!

!Command: config
 int eth 0/5
 channel-group 10 mode active type standard
 no shut
!Time: Mon Aug 22 18:33:04 2016


!Command: show running-config int eth 0/5
!Time: Mon Aug 22 18:33:05 2016

interface Ethernet 0/5
 channel-group 10 mode active type standard
 lacp timeout long
 no shutdown
!

<output truncated>
```

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"}
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Enter an integer from 0 through 6.

Modes

Interface subtype configuration mode

Usage Guidelines

When Interface ingress QoS Trust is in the un-trusted mode, then the Interface Default CoS value is applied to all ingress traffic for user priority mapping. When the interface ingress QoS Trust is in the CoS mode, then the Interface Default CoS value is applied to all nonpriority tagged ingress traffic for user priority mapping.

If the interface is QoS trusted, the CoS value of the interface is used to assign a CoS value to all untagged packets entering the interface.

QoS Trust is implicitly turned on when the QoS CoS-Mutation map is applied to interfaces, and is implicitly turned off when the QoS CoS-Mutation map is removed.

Examples

To set the CoS value to 2 on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/3
device(conf-if-eth-0/3)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos cos-mutation

Applies a user configured QoS CoS-to-CoS mutation map to an interface.

Syntax

qos cos-mutation *cos_map_name*

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.

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 0/3
device(conf-if-eth-0/3)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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 0/3
device(conf-if-eth-0/3)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos cpu

Accesses Quality of Service (QoS) central processing unit (CPU) configuration mode to configure the frame rate on the CPU queues mapped to the protocols for the device.

Syntax

qos cpu

no qos cpu

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the default frame rate for all CPU queues.

Examples

The following example accesses QoS CPU configuration mode.

```
device# configure terminal
device(config)# qos cpu
device(config-qos-cpu)#
```

History

Release version	Command history
17s.1.01	This command was introduced.

qos drop-monitor enable

Enables RASlog drop monitioring for ingress port drops and egress queue drops.

Syntax

qos drop-monitor enable

no qos drop-monitor enable

Command Default

QoS drop monitoring is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

The drop-polling interval is 60 seconds. If drops occur during this interval, a RASlog message is generated.

Use the **no** form of this command to disable drop monitoring.

Examples

The following example enables RASlog drop monitioring for ingress port drops and egress queue drops.

```
device# configure terminal
device(config)# interface Ethernet 0/2
device(conf-if-eth-0/2)# qos drop-monitor enable
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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.

The dscp-cos map needs to applied on the ingress interface. It is effective only when the dscp-traffic-class and dscp-mutation maps are also applied to same interface.

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 0/2
device(conf-if-eth-0/2)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos dscp-mutation

Applies a 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.

The dscp-mutation map needs to applied on the ingress interface. It is effective only when the dscp-cos and dscp-traffic-class maps are also applied to same interface.

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 0/3
device(conf-if-eth-0/3)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

The dscp-traffic-class map needs to applied on the ingress interface. It is effective only when the dscp-cos and dscp-mutation maps are also applied to same interface.

Examples

Follow this example to apply a QoS DSCP-to-traffic class mutation map to a specific Ethernet interface

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos flowcontrol

Activates and configures QoS flow control.

Syntax

qos flowcontrol tx { **on** | **off** } **rx** { **on** | **off** }

no qos flowcontrol

Command Default

By default, QoS flow control is disabled for both directions.

Parameters

tx { **on** | **off** }

Activates or deactivates the transmission portion of flow control.

rx { **on** | **off** }

Activates or deactivates the receiving portion of flow control.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no qos flowcontrol** to deactivate flow control on a specific interface.

When a receiving device is congested, it communicates with the transmitting device by sending a PAUSE frame that instructs the device to stop data transmission for a specified period of time. This feature is available per port in all front ports and applies to all the traffic on the link. However, the SLX-OS devices support the receive direction only. These devices supports pause flow control and priority flow control.

Examples

The following example activates both the transmitting and receiving portions of flow control on the Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/6
device(conf-if-eth-0/6)# qos flowcontrol tx on rx on
```

The following example disables flow control on a port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 33
device(config-Port-channel-33)# no qos flowcontrol
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map cos-dcsp

Creates a QoS CoS-to-DSCP map for the mapping of the ingress CoS value to outgoing DSCP values.

Syntax

qos map cos-dcsp *name*

no qos map cos-dcsp *name*

Parameters

name

Specifies the name of CoS-to-DSCP map.

Modes

Global configuration mode

Usage Guidelines

This map can be used in a remarking profile only. It cannot be applied directly to an interface.

Use the **no** form of the command to remove the map.

Examples

The following example creates a QoS CoS-to-DSCP map.

```
device# configure terminal
device(config)# qos map cos-dscp test1
device(cos-dscp-test1)#
```

The following example removes a QoS CoS-to-DSCP map.

```
device# configure terminal
device(config)# no qos map cos-dscp test1
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map cos-mutation

Creates a QoS CoS-to-CoS mutation map.

Syntax

qos map cos-mutation *name*

no qos map cos-mutation *name*

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.

Modes

Global configuration mode

Usage Guidelines

Use the **no** of this command to delete the QoS CoS-to-CoS mutation map.

A QoS map can only be deleted if it is not bound to any interface.

Both cos-mutation and cos-traffic class maps must be applied on a port, otherwise the map configuration is not active. If you want to have a user-defined cos-mutation configuration and default cos-traffic class configuration on a port, you must explicitly apply the default cos-traffic class map on a port, otherwise the cos-mutation configuration is not active.

Examples

The following example creates a CoS-to-CoS QoS mutation map.

```
device# configure terminal
device(config)# qos map cos-mutation cosMap
```

The following example deletes a CoS-to-CoS QoS mutation map.

```
device# configure terminal
device(config)# no qos map cos-mutation cosMap
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map cos-traffic-class

Creates 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.

Both cos-mutation and cos-traffic class maps must be applied on a port, otherwise the map configuration is not active. If you want to have a user-defined cos-mutation configuration and default cos-traffic class configuration on a port, you must explicitly apply the default cos-traffic class map on a port, otherwise the cos-mutation configuration is not active.

Enter **no** form of the command to delete the named QoS CoS-to-traffic class mutation map.

A QoS map can only be deleted if it is not bound to an interface.

Examples

To create a QoS CoS-to-traffic class mutation map use the following command

```
device# configure terminal
device(config)# qos map cos-traffic-class cosTC1
```

To delete a QoS CoS-to-traffic class mutation map that is bound to an interface follow this example.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no qos cos-traffic-class cosTC1
device(conf-if-eth-0/1)# exit
device(config)# no qos map cos-traffic-class cosTC1
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map dscp-cos

Creates a QoS DSCP-to-CoS map for the mapping of the ingress DSCP value to outgoing 802.1P values.

Syntax

qos map dscp-cos *name*

no qos map dscp-cos *name*

Parameters

name

Name of DSCP-to-CoS map

Modes

Global configuration mode

Usage Guidelines

This command remaps the incoming DSCP values of the ingress packet to egress CoS 802.1P values.

All DSCP map types must be applied on a port, otherwise the map configuration is not active. If you want to have default configuration on a port for one of the Layer 3 maps, you must explicitly apply the default configuration of the Layer 3 map type.

Use the **no** form of the command to remove the DSCP-to-CoS map.

Examples

The following example creates a QoS DSCP-to-CoS map.

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)#
```

The following example removes a QoS DSCP-CoS map.

```
device# configure terminal
device(config)# no qos map dscp-cos test
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map dscp-mutation

Creates a DSCP mutation map for mapping the incoming DSCP value of the ingress packet to outgoing DSCP values.

Syntax

qos map dscp-mutation *name*

no qos map dscp-mutation *name*

Parameters

name

Specifies the name of the DSCP mutation map.

Modes

Global configuration mode

Usage Guidelines

After you create the DSCP mutation map, you can map ingress DSCP values to egress DSCP values using the **map dscp** command.

All DSCP map types must be applied on a port, otherwise the map configuration is not active. If you want to have default configuration on a port for one of the Layer 3 maps, you must explicitly apply the default configuration of the Layer 3 map type.

Use the **no** form of this command to delete this map.

Examples

The following example creates a QoS DSCP mutation map.

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)#
```

The following example removes a QoS DSCP mutation map.

```
device# configure terminal
device(config)# no qos map dscp-mutation test
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map dscp-traffic-class

Creates a QoS map for performing DSCP-to-traffic class mapping.

Syntax

qos map dscp-traffic-class *name*

no qos map dscp-traffic-class *name*

Command Default

DSCP-to-traffic class mutation is not enabled.

Parameters

name

Name of the QoS DSCP-to-traffic class map.

Modes

Global configuration mode

Usage Guidelines

After you configure the QoS DSCP-to-Traffic-Class map, you can map the ingress DSCP values to a traffic class value using the **map** command.

All DSCP map types must be applied on a port, otherwise the map configuration is not active. If you want to have default configuration on a port for one of the Layer 3 maps, you must explicitly apply the default configuration of the Layer 3 map type.

Enter **no qos dscp-traffic-class** *name* while in the interface mode to remove the map from that interface.

Examples

The following example creates a QoS DSCP-to-traffic class map.

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)#
```

The following example removes a QoS DSCP-traffic class map.

```
device# configure terminal
device(config)# no qos map dscp-traffic-class test
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map traffic-class-cos

Creates a QoS traffic-class-to-CoS map.

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.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to delete the map.

This map can only be used in a remark profile and cannot be applied on interface.

Examples

The following example creates a QoS traffic class-to-CoS mutation map.

```
device# configure terminal
device(config)# qos map traffic-class-cos CoSMap
device(traffic-class-cos-CoSMap)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map traffic-class-dscp

Creates a QoS map for performing traffic class-to-DSCP mapping.

Syntax

qos map traffic-class-dscp *name*

no qos map traffic-class-dscp *name*

Parameters

name

Specifies the name of the QoS traffic-class-to-DSCP map.

Modes

Global configuration mode

Usage Guidelines

After you configure the QoS traffic-class-to-DSCP map, you can map the ingress traffic class values to a DSCP value using the **map traffic-class** command.

This map can be used in a remarking profile only. It cannot be applied directly to an interface.

Use the **no** form of this command to delete the map.

Examples

The following example creates a QoS traffic-class-to-DSCP map.

```
device# configure terminal
device(config)# qos map traffic-class-dscp test
device(traffic-class-dscp-test)#
```

The following example removes a QoS traffic-class-to-DSCP map.

```
device# configure terminal
device(config)# no qos map traffic-class-dscp test
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos map traffic-class-mutation

Creates a traffic-class mutation map for mapping the incoming traffic class value of the ingress packet to outgoing traffic class value.

Syntax

qos map traffic-class-mutation *name*

no qos map traffic-class- *name*

Parameters

name

Specifies the name of the traffic-class mutation map.

Modes

Global configuration mode

Usage Guidelines

After you create the traffic-class mutation map, you can map ingress traffic-class values to egress traffic-class values using the **map traffic-class** command.

This map can only be used in a remark profile and cannot be applied on interface.

Use the **no** form of this command to delete the map.

Examples

The following example creates a QoS traffic-class mutation map.

```
device# configure terminal
device(config)# qos map traffic-class-mutation test
device(traffic-class-mutation-test)#
```

The following example removes a QoS traffic-class mutation map.

```
device# configure terminal
device(config)# no qos map traffic-class-mutation test
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos random-detect traffic-class

Maps a Random Early Detect (RED) profile to a CoS priority value for a port.

Syntax

qos random-detect traffic-class *value* **red-profile-id** *profile-ID value*

no qos random-detect traffic-class *value*

Command Default

Port CoS priority value is not mapped to the RED profile.

Parameters

value

Class of Service (COS) value. Valid values range from 0 through 7.

profile-ID value

Random Error Detection value. Valid values range from 1 through 384.

Modes

Interface subtype configuration mode

Usage Guidelines

The RED profile is defined by the **qos red-profile** command.

Enter **no qos random-detect traffic-class** *value* while in the interface mode to remove the DSCP-to-Traffic-Class map from the interface.

Examples

The following example maps the profile to CoS priority 7 on a Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-0/2)# qos random-detect traffic-class 7 red-profile-id 2
```

The following example removes the previously created profile from the interface:

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-0/2)# no qos random-detect traffic-class 7
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos red profile

Creates a Random Early Detect (RED) profile for egress traffic flow and provides a minimum threshold, maximum threshold, and drop-probability for egress traffic flow.

Syntax

qos red-profile *profile-ID* **min-threshold** *percentage* **max-threshold** *percentage* **drop-probability** *percentage*

no qos red-profile *profile-ID*

Parameters

profile-ID
Specifies the profile ID. Enter an integer from 1 through 384.

min-threshold *percentage*
Specifies the minimum threshold in percentage of queue size for randomly dropping packets. Enter an integer from 0 through 100.

max-threshold *percentage*
Specifies the maximum threshold in percentage of queue size when packets are dropped with 100% probability. Enter an integer from 0 through 100.

drop-probability *percentage*
Specifies the probability in percentage that packets will be dropped when minimum threshold is reached. Enter an integer from 0 through 100.

Modes

Global configuration mode

Usage Guidelines

Enter **qos random-detect cos** command while in configuration mode for a specific interface to map the profile to a CoS priority for a port.

Enter **no qos random-detect cos** command in the interface mode to remove the profile from the interface. You must remove the profile from interface before you can remove the profile itself.

Use the **no** form of this command to remove the profile.

Examples

The following example creates a RED profile.

```
device# configure terminal
Entering configuration mode terminal
device(config)# qos red-profile 2 min-threshold 10 max-threshold 80 drop-probability 80
```

The following example removes the profile.

```
device# configure terminal
device(config)# no qos red-profile 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos trust

Configures QoS CoS or DSCP trust on an interface.

Syntax

qos trust { **cos** | **dscp** }

no qos trust { **cos** | **dscp** }

Command Default

Both CoS and DSCP trust are disabled on the interface.

Parameters

cos

Enables CoS trust on the interface to honor the incoming CoS value of the ingress packet.

dscp

Enables DSCP trust on the interface to honor the incoming IP DSCP settings for deciding the queue priority value of the ingress packet.

Modes

Interface type configuration mode

Usage Guidelines

Use the **no** form of this command to disable CoS or DSCP trust on the interface.

When DSCP trust is not enabled, the DSCP value in the packet is ignored.

When Layer 2 maps are active on an interface, CoS on this interface is trusted implicitly.

Examples

The following example enables CoS trust on an interface.

```
device# configure terminal
device(config)# interface Ethernet 0/6
device(conf-if-eth-0/6)# qos trust cos
```

The following example enables DSCP trust on an interface.

```
device# configure terminal
device(config)# interface Ethernet 0/2
device(conf-if-eth-0/2)# qos trust dscp
```

History

Release version	Command history
17s.1.00	This command was introduced.

qos tx-queue limit

Limits the buffer usage for egress lossy unicast queues.

Syntax

qos tx-queue limit *queue-limit*

no qos tx-queue limit

Command Default

The default limit is 512 Kbytes.

Parameters

queue-limit

Specifies the egress queue limit in Kbytes. Enter an integer from 128 to 8000.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to reset the default limit of 512 Kbytes.

The recommended egress queue limit is 128 to 2000 Kbytes.

The size of the shared buffer pool on the ExtremeSwitching SLX 9140 is 14,615 pages and the ExtremeSwitching SLX 9240 is 37,143 pages, where each page is a size of 256 bytes.

When setting the TX-queue limit, the queue limit is set to one of the following values (the next higher value above the configured value). For example, if you configure the value to 512 Kbytes, the queue limit is set to 748288 bytes on the SLX 9140 or 570368 bytes on the SLX 9240.

Examples

The following example limits the buffer usage for egress lossy unicast queues to 256 Kbytes.

```
device# configure terminal
device(config)# qos tx-queue limit 256
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

traffic_class

There are eight traffic class values:

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:

1

Traffic class 0 DWRR weight.

2

Traffic class 1 DWRR weight.

3
Traffic class 2 DWRR weight.

4
Traffic class 3 DWRR weight.

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

Use the **no** form of the command to remove the SP value for the egress queue traffic class scheduler.

Examples

The following example assigns 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

queue

Selects the CPU queue and accesses Quality of Service (QoS) central processing unit (CPU) queue configuration mode to configure the queue rate.

Syntax

queue *queue-number*

no queue

Parameters

queue-number

Specifies the number of the queue. The number of queues is dependent on the device. For the SLX 9140 or SLX 9240 device, enter an integer from 0 through 31.

Modes

QoS CPU configuration mode

Usage Guidelines

Use the **show qos cpu queue info** command to display the mapping of all CPU queues to the protocols.

The **no** form of the command removes the queue from the QoS CPU configuration and resets the queue to its default frame rate value.

Examples

The following example selects queue 2 and accesses QoS CPU queue configuration mode for its rate configuration.

```
device# configure terminal
device(config)# qos cpu
device(config-qos-cpu)# queue 2
device(config-qos-cpu-queue-2)#
```

History

Release version	Command history
17s.1.01	This command was introduced.

Commands R - Sh

radius-server host

Specifies a Remote Authentication Dial-In User Service (RADIUS) server, including the VRF to use for communication with the server, and enters RADIUS server host VRF configuration mode.

Syntax

radius-server host { *ip-address* | *host_name* } [**use-vrf** [*vrf-name*]]

no radius-server host { *ip-address* | *hostname* } [**use-vrf** [*vrf-name*]]

Command Default

A RADIUS server is not configured.

Parameters

ip-address

Specifies the RADIUS server host in IP address format. Both IPv4 or IPv6 address formats are supported.

host_name

Specifies the RADIUS server host in hostname format. A hostname can be up to 40 characters in length.

use-vrf

(Optional) Specifies using a specific VRF for communication with the RADIUS server and enters configuration mode for the RADIUS server host VRF.

vrf-name

(Optional) Specifies a VRF. By default and when a VRF is not specified, the management VRF (mgmt-vrf) is used for communication with the RADIUS server.

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 radius-server host** command removes the RADIUS server 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.

Examples

The following example shows how to configure a RADIUS server on a device. The IP address of the RADIUS server is 10.24.65.6.

```
device# configure terminal
device(config)# radius-server host 10.24.65.6
device(config-radius-server-10.24.65.6/mgmt-vrf)#
```

The following example shows how to configure a RADIUS server (with an IP address 10.24.65.6) and specify using the green-vrf for communication with this server. Specifying the **use-vrf** option enters configuration mode for the RADIUS server host 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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

rate-limit

Sets the rate limit for the central processing unit (CPU) queue.

Syntax

rate-limit *fps*

no rate-limit

Command Default

The default value is dependent on the CPU queue. Refer to the table in the Usage Guidelines.

Parameters

fps

Specifies the rate as frames per second (FPS). Enter an integer from 0 through 10000.

Modes

QoS CPU queue configuration mode

Usage Guidelines

Use the **show qos cpu queue info** command to view the frames per second for each queue and the mapping of the queue to the protocol.

If you enter a frame rate that exceeds the unused credits displayed by the **show qos cpu queue info** command, an error message is displayed. You must reduce the rate for another queue to increase the available unused credits.

Some protocol CPU queues have a maximum rate, as listed in the following table.

TABLE 5 CPU queue, associated protocol, and FPS

CPU queue	Protocols	Default FPS	Maximum FPS
0	sFlow	1000	3096
1	ACL logging	256	2048
2	Subnet trap (LPM hit, LPM miss)	256	512
3	Unused/reserved for future use	4096	—
4	SA and DA MAC learning	8192	10000
5	Unused/reserved for future use	384	—
6	DAI	64	10000
7	All device IP traffic except Telnet, SSH, and ping (MyIP)	300	8192
8	ARP suppression request, ARP request, VRRP ARP request, VRRP ARP suppression request, ND request	384	10000
9	Router solicitations	128	10000
10	IGMP	512	10000

TABLE 5 CPU queue, associated protocol, and FPS (continued)

CPU queue	Protocols	Default FPS	Maximum FPS
11	PIM	256	10000
12	MLD	256	10000
13	DHCP relay request	1500	10000
14	Telnet and SSH to the device IP address (MyIP Telnet, MyIP SSH)	512	8192
15	Unused	NA	NA
16	OSPF	1500	10000
17	BGP	1500	10000
18	ARP response, ND response	768	10000
19	DHCP relay response	1500	10000
20	VRRP, VRRP-E	2048	10000
21	ICMP and ping to device IP address (MyIP Ping)	32	1024
22	Unused/reserved for future use	128	—
23	802.1X (dot1x)	256	256
24	LLDP	128	128
25	PTP	512	1024
26	CTP	1024	2048
27	BFD	2048	5120
28	Unused/reserved for future use	256	—
29	Unused/reserved for future use	128	—
30	STP and PVST	2176	2176
31	LACP	128	128

Use the **no** form of the command to reset the default rate limit for the queue.

Examples

The following example configures the rate limit for the specified CPU queue.

```
device# configure terminal
device(config)# qos cpu
device(config-qos-cpu)# queue 2
device(config-qos-cpu-queue-2)# rate-limit 512
```

History

Release version	Command history
17s.1.01	This command was introduced.

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

EVPN instance configuration mode

EPVN VLAN/BD configuration mode

Usage Guidelines

Examples

The following example configures an RD and assigns the local ASN number 200:1.

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# 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-myinstance)# bridge-domain 200
device(config-bridge-domain-200)# rd 10.1.1.1:1
```

History

Release version	Command history
17s.1.01	This command was introduced.

redistribute

Configures the device to redistribute IPv4 and IPv6 routes from one routing domain to another.

Syntax

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*]

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

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 *num*
Specifies a metric for redistributed routes. Range is from 1 through 65535 in OSPFv2 and OSPFv3 configuration mode. Range is from 1 through 4261412863 in BGP address-family IPv4/IPv6 unicast configuration mode.

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.

route-map *string*
Specifies a route map to be consulted before a route is added to the routing table.

ospf
Specifies the OSPF protocol.

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

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

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 and OSPFv3 router VRF configuration mode.

The **match**, **metric**, and **metric-type** options are not available in OSPF VRF configuration mode.

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 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 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 region-1:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# region region-1
```

History

Release version	Command history
17s.1.00	This command was introduced.

reload

Reboots the standby or chassis or triggers a power-cycle of the switch and automatically reboot the switch into offline diagnostic mode.

Syntax

reload { **diag-mode** | **system** }

Parameters

diag-mode

Power-cycle the switch and automatically reboot the switch into offline diagnostic mode.

system

Reboots the chassis.

Modes

Privileged EXEC mode

Usage Guidelines

The diagnostic functionalities are provided in offline diagnostic mode by DiagOS. The offline diagnostic utility, DiagOS, runs in a separate mode and context from SLX-OS. To enter offline diagnostic mode from the SLX-OS command prompt, enter the **reload diag-mode** command in privileged EXEC mode.

After the **reload diag-mode** command is executed, the offline diagnostic mode is preserved persistently on the switch for the subsequent reboots and power-cycles. To exit offline diagnostic mode and return to SLX-OS mode, enter the **reload slxos-mode** command from the offline diagnostic prompt as follows:

```
diag<~>#  reload slxos-mode
device#
```

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 system** command performs a cold reboot that powers off and restarts the entire chassis. All session connections must be restarted. If the power-on self-test (POST) is enabled, POST is executed when the system comes back up.

NOTE

Do not use the **reload** command without either the **diag-mode** or **system** parameter.

Examples

The following example performs a cold reboot of the device.

```
device# reload system
```

The following example power-cycles the switch and automatically reboots the switch into offline diagnostic mode.

```
device# reload diag-mode
Warning: This operation will cause the switch to power cycle and
go to offline diagnostic mode after reboot.
All existing telnet, secure telnet and SSH session will be terminated

Are you sure you want to proceed to reboot the switch [y/n]? y
```

History

Release version	Command history
17s.1.00	This command was introduced.

reload (DiagOS)

Triggers a power cycle of the switch.

Syntax

reload [**diag** | **slxos-mode**]

Command Default

The default without an option is **reload**, which has the same effect as **reload diag**.

Parameters

diag

Power-cycles the switch and reboots back to offline diagnostics mode.

slxos-mode

Power-cycles the switch and reboots to SLX-OS mode.

Modes

Offline diagnostic mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

Use the **reload slxos-mode** command to power cycle the switch and return to SLX-OS mode once the offline diagnostic testing is completed. Otherwise, use **reload diag** command to power cycle the switch after each test. Power cycling is required to clean up the system before the next test case can be run.

ATTENTION
Wait for the system to reload automatically, as this process can take some time to complete.

Examples

The following example power cycles the system and re-enters SLX-OS mode.

```
diag<~>#  reload slxos-mode
power restart
DRAM Init-DDR3
CBR0-12345670123456701234567012345670
CBR134Done
```

History

Release version	Command history
17s.1.00	This command was introduced.

remap lossless-priority

Configures the Class of Service (CoS) to be remapped for the lossless priority.

Syntax

remap lossless-priority priority *CoS-value*

no remap lossless-priority priority

Command Default

The default CoS value is 0.

Parameters

priority *CoS-value*

Specifies the CoS value. Enter an integer from 0 to 6.

Modes

CEE map configuration mode

Usage Guidelines

Use the **no** form for this command to reset the default CoS value of 0.

Examples

The following example configure the lossless priority to 2.

```
device# configure terminal
device(config)# cee-map default
device(config-cee-map-default)# remap lossless-priority priority 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

remove destination

Removes one or more destinations from a policy-based forwarding (PBF) destination-group.

Syntax

remove destination *destination-id*

Command Default

Destinations that were added are contained in the PBF destination group.

Parameters

destination-id

Specifies one or more PBF destination IDs. You can specify one ID, a range (example: 3-5), a comma-separated list (example: 1,3,5,6), or combine IDs, ranges, and lists (example: 1-5,6,8).

Modes

PBF destination-group configuration mode

Usage Guidelines

To remove all destinations from a PBF destination-group, you can also use the **no add destination** command.

Examples

The following example add a range of destinations to a PBF destination-group and then removes specific destinations.

```
device# configure terminal
device(config)# pbf destination-group 171
device(config-destination-group-171)# add destination 10,20-30
device(config-destination-group-171)# remove destination 21,25
device(config-destination-group-171)# do show running-config pbf destination-group 171
   pbf destination-group 171
   add destination 10,20,22-24,26-30
!
```

History

Release version	Command history
18s.1.02	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 4294967290.

increment
Specifies a value to increment the sequence number between rules. Valid values range from 1 through 4294967290.

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
!
```

resource-monitor cpu enable

Enables the CPU utilization monitoring service.

Syntax

resource-monitor cpu enable [**action** { **raslog** | **streaming** | **both** }] [**threshold** *percentage*]

no resource-monitor cpu enable

Command Default

Default action is to set to generate RASlog messages when CPU usage exceeds the threshold of 90%.

Parameters

action { **raslog** | **streaming** | **both** }

Action to take when CPU usage exceeds threshold. Valid output options are RASlog, streaming, or both.

threshold *percentage*

Threshold for high CPU usage. The range of valid values is from 70 through 90 percent.

Modes

Configuration mode

Usage Guidelines

This is a node-specific command.

The **no** form of the command disables the CPU utilization monitoring.

Examples

The following example disables the CPU utilization monitoring service.

```
device# configure terminal
device(config)# no resource-monitor CPU enable
```

The following example re-enables the CPU utilization monitoring service if it has been disabled.

```
device# configure terminal
device(config)# resource-monitor CPU enable action raslog threshold
```

History

Release version	Command history
17s.1.00	This command was introduced.

resource-monitor memory enable

Enables the memory utilization monitoring service.

Syntax

resource-monitor memory enable [**action** { **raslog** | **streaming** | **both** }] [**threshold** *percentage*]

no resource-monitor memory enable

Command Default

Default action is to set to generate RASlog messages when memory usage exceeds the threshold of 90%.

Parameters

action { **raslog** | **streaming** | **both** }

Action to take when memory usage exceeds threshold. Valid output options are RASlog, streaming, or both.

threshold *percentage*

Threshold for high memory usage. The range of valid values is from 70 through 90 percent.

Modes

Configuration mode

Usage Guidelines

This is a node-specific command.

The **no** form of the command disables the memory utilization monitoring.

Examples

The following example disables the memory utilization monitoring service.

```
device# configure terminal
device(config)# no resource-monitor memory enable
```

The following example re-enables the memory utilization monitoring service if it has been disabled.

```
device# configure terminal
device(config)# resource-monitor memory enable action raslog threshold
```

History

Release version	Command history
17s.1.00	This command was introduced.

resource-monitor process memory

Configures the per-process memory monitoring service.

Syntax

resource-monitor process memory alarm *alarm_threshold* [**critical** *critical_threshold*] [**enable**]

resource-monitor process memory enable [**alarm** *alarm_threshold*] [**critical** *critical_threshold*]

resource-monitor process memory critical *critical_threshold* [**alarm** *alarm_threshold*] [**enable**]

no resource-monitor process memory enable

Command Default

This command is enabled by default.

Parameters

alarm *alarm_threshold*

Specifies the alarm threshold, crossing which, specific RASlog is generated. Valid values range between 500 to 599 MB. The default is 500.

enable

Enables the pre-process memory monitoring service.

critical *critical_threshold*

Specifies the critical threshold, crossing which, specific RASlog is generated. Valid values range between 600 to 699 MB. The default is 600.

Modes

Global configuration mode

Usage Guidelines

This is a node-specific command. When the alarm threshold is reached, it generates the RASlog message SRM-1003. When the critical threshold is reached, it generates the RASlog message SRM-1004.

The **no** form of the command disables the pre-process memory monitoring on CPU.

Examples

The following example enables the pre-process memory monitoring service and sets an alarm threshold of 550 MB and a critical threshold of 620 MB.

```
device# configure terminal
device (config)# resource-monitor process memory enable alarm 550 critical 620
```

History

Release version	Command history
17s.1.00	This command was introduced.

retain route-target all

Enables BGP to retain all EVPN routes in the EVPN routing table.

Syntax

retain route-target all

no retain route-target all

Command Default

This functionality is disabled.

Modes

Address-family L2VPN EVPN configuration mode

Usage Guidelines

Use the **no** form of this command to disable this functionality.

Examples

To retain all EVPN routes:

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# retain route-target all
```

History

Release version	Command history
17s.1.01	This command was introduced.

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 retries** command restores the 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

retries (Telemetry)

Defines the number of retry attempts allowed to contact the LDAP host.

Syntax

retries { *num* }

no retries

Command Default

The retry value 5.

Parameters

retries

Specifies the number of retries for the server connection. The range is 0 through 100.

Modes

LDAP host configuration mode.

Usage Guidelines

Use the no form of this command to remove the retry value.

Examples

To add an LDAP server with retries set to three:

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# retries 3
```

Executing **no** on an attribute sets it with its default value.

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# no retries
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Enter **no revision** to return to the default setting.

Examples

To set the configuration revision to 1:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# revision 1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

The **no** form of the command disables 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Any number of RIB routes can be installed in the RTM.

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.

The **no** form of the command removes the configured maximum number of RIB routes allowed.

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 in 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)# rib-route-limit 32000
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 *index snmp_oid*

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, where 65535 is rmon collection stats index on a given interface. 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 15.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

rmon collection history

Collects Ethernet group statistics at specified interval for later retrieval.

Syntax

rmon collection history *number* [**buckets** *bucket_number* | **interval** *seconds* | **owner** *name*]

no rmon 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 0/6
device(conf-if-eth-0/6)# rmon collection history 5 owner admin
```

History

Release version	Command history
17s.1.00	This command was introduced.

rmon collection stats

Collects Ethernet group statistics on 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 0/6
device(conf-if-eth-0/6)# rmon collection stats 2 owner admin
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 *index*

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 15 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

route-map (default system-mode)

Creates a route map; for an existing route map, adds a stanza.

Syntax

route-map *name* { **permit** | **deny** } *stanza*

no route-map *name* { **permit** | **deny** } *stanza*

Parameters

name

Specifies the name of the route map. Names range from 1 through 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.

Modes

Global configuration mode

Usage Guidelines

This command is used with the **match** and **set** commands.

The **continue** command configures the route map to continue to evaluate and run 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

route-map (NPB)

Creates a route map; for an existing route map, adds a stanza.

Syntax

route-map *name* { **permit** | **deny** } *stanza*

no route-map *name* { **permit** | **deny** } *stanza*

Parameters

name

Specifies the name of the route map. Names range from 1 through 63 ASCII characters in length.

permit

Enables the **set** statement within the specified stanza, as specified in the Usage Guidelines.

deny

Disables the **set** statement within the specified stanza, as specified in the Usage Guidelines.

stanza

Specifies the stanza ID. Valid values range from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

The following table describes the interactions between route-map **permit** and **deny** stanzas and **permit** and **deny** rules in ACLs applied to those stanzas by **match { mac | ip | ipv4 | uda } address acl** statements.

TABLE 6 Stanza and ACL **permit** and **deny** interactions

Stanza	ACL rule	Resulting TCAM action
Permit	Permit	The **set** statement or statements are applied.
Permit	Deny	Packets that match a **deny** keyword are denied from using the stanza **set** statement: • NPB: The packet is dropped. • PBR: The packet is routed as normal.
Deny	Permit	No action is taken: • NPB: The packet is dropped. • PBR: The packet is routed as normal.
Deny	Deny	If there are no subsequent matches, the packet is forwarded.

The **no** form of this command deletes a route-map stanza.

Examples

The following example enables the NPB route map for an Ethernet interface so that all ingress traffic from interface Ethernet 0/1 exits from port-channel 100. The absence of a **match** statement is treated as "match any"; all traffic is forwarded according to the **set** statement.

```
device# configure terminal
device(config)# route-map npb_map permit 10
device(config-route-map-npb_map/permit/10)# set interface port-channel 100
device(config-route-map-npb_map/permit/10)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# npb policy route-map npb_map
```

The following example configures ingress traffic from Ethernet 0/1 and port-channel 100 to egress Ethernet 0/5.

```
device# configure terminal
device(config)# route-map npb_map permit 10
device(config-route-map-npb_map/permit/10)# match ip address acl acl_2
device(config-route-map-npb_map/permit/10)# set interface ethernet 0/5
device(config-route-map-npb_map/permit/10)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# npb policy route-map npb_map
device(conf-if-eth-0/1)# exit
device(config)# interface port-channel 100
device(config-Port-channel-100)# npb policy route-map npb_map
```

The following example replicates traffic entering an interface to multiple egress interfaces.

```
device# configure terminal
device(config)# tvf-domain 10
device(config-tvf-domain-10)# description Sample TVF description
device(config-tvf-domain-10)# exit
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# tvf-domain add 10
device(conf-if-eth-0/5)# exit
device(config)# interface port-channel 10
device(config-Port-channel-10)# tvf-domain add 10
device(config-Port-channel-10)# exit
device(config)# route-map npb_map1 permit 1
device(config-route-map-npb_map1/permit/1)# match ip address acl acl_2
device(config-route-map-npb_map1/permit/1)# set next-hop-tvf-domain 5
device(config-route-map-npb_map1/permit/1)# exit
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# npb policy route-map npb_map1
```

The following two-stanza route-map forwards frames according to the following conditions: Stanza 10 examines whether a frame matches the specified ACL; a match forwards the frame to port 0/21. If 0/21 is not up, the frame is forwarded to port-channel 666. If the Stanza 10 conditions are not met, Stanza 20 is examined. Because there is no match statement, it is considered a “match any”. All such traffic is forwarded to TVF domain 100—if it contains at least one interface and at least one of its member ports is up. If TVF 100 is not up, traffic is forwarded to interface 0/21, if up.

```
device# configure terminal
device(config)# route-map pbrTest permit 10
device(config-route-map-pbrTest/permit/10)# match ip address acl acl_pbr_05
device(config-route-map-pbrTest/permit/10)# set interface eth 0/21
device(config-route-map-pbrTest/permit/10)# set interface port-channel 666
device(config-route-map-pbrTest/permit/10)# exit

device(config)# route-map pbrTest permit 20
device(config-route-map-pbrTest/permit/20)# set next-hop-tvf-domain 100
device(config-route-map-pbrTest/permit/20)# set interface eth 0/21
```

The following NPB-grid example creates destination 5 within destination group 99. It then configures ingress traffic from Ethernet 0/1 and port-channel 100 to destination group 99.

```
device# configure terminal
device(config)# pbf destination 5
device(config-destination-5)# statistics-enable
device(config-destination-5)# precedence 10 set interface eth 0/12:3
device(config-destination-5)# exit
device(config)# pbf destination-group 99
device(config-destination-group-99)# add destination 5
device(config-destination-group-99)# exit

device(config)# route-map npb_map permit 10
device(config-route-map-npb_map/permit/10)# set interface pbf-destination-group 99
device(config-route-map-npb_map/permit/10)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# npb policy route-map npb_map
device(conf-if-eth-0/1)# exit
device(config)# interface port-channel 100
device(config-Port-channel-100)# npb policy route-map npb_map
```

History

Release version	Command history
17s.1.01	This command was introduced.

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 instance configuration mode

EPVN 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 myinstance
device(config-evpn-myinstance)# bridge-domain 200
device(config-bridge-donain-200)# route-target both 200:1
```

History

Release version	Command history
17s.1.01	This command was introduced.

router bgp

Enables BGP routing.

Syntax

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 VRFconfiguration 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)
```

History

Release version	Command history
17s.1.00	This command was introduced.

router-interface

Attaches (binds) a router interface to a VLAN, creating a Layer 3 interface.

Syntax

router-interface ve *vlan_ID*

no router-interface ve

Command Default

A router interface is not configured.

Parameters

ve *vlan_ID*
Specifies a VLAN ID.

Modes

VLAN configuration mode

Usage Guidelines

Only one router VE interface can be mapped to a VLAN.

The VLAN ID and the VE ID need not be the same.

Use the **no** form of the command to remove the router interface from the VLAN.

Examples

To attach a router interface to a Layer 2 VLAN:

```
device(config)# vlan 2
device(config-vlan-2)# router-interface ve 2
```

To remove the router interface:

```
device(config)# vlan 2
device(config-vlan-2)# no router-interface ve
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

seq (deny/permit rules in UDAs)

Inserts filtering rules into user-defined ACLs (UDAs).

Syntax

seq *seq-value* { **deny** | **permit** } *uda-value-0 mask-0 uda-value-1 mask-1 uda-value-2 mask-2 uda-value-3 mask-3* [**count**] [**log**]

no seq *seq-value*

{ **deny** | **permit** } *uda-value-0 mask-0 uda-value-1 mask-1 uda-value-2 mask-2 uda-value-3 mask-3* [**count**] [**log**]

no { **deny** | **permit** } *uda-value-0 mask-0 uda-value-1 mask-1 uda-value-2 mask-2 uda-value-3 mask-3* [**count**] [**log**]

Command Default

The concluding, default rule is deny.

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.

deny
Specifies rules to deny traffic.

permit
Specifies rules to permit traffic.

uda-value-0, *uda-value-1*, *uda-value-2*, *uda-value-3*
Specifies the hex values with which traffic is matched, at the offsets defined in the UDA profile.

mask-0, *mask-1*, *mask-2*, *mask-3*
Specifies hex-value masks for the UDA values.

count
Enables statistics for the rule.

log
Enables inbound logging for the rule.

Modes

UDA configuration mode

Usage Guidelines

Ths command is supported only in NPB system mode.

If there is no matching rule, the frame is permitted.

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*.

Examples

The following example creates a UDA and defines a permit rule.

```
device# configure terminal
device(config)# uda access-list extended uda_acl_1
device(conf-uda-acl-ext)# permit 0x112233 0xFFFFFF 0x0a0a0001 0xFFFFFFFF 0x0a0b0001 0xFFFFFFFF
0x11223344 0xFFFFFFFF
```

History

Release version	Command history
18s.1.00	This command was introduced.

seq (overlay class map)

Adds or deletes a tunnel classification.

Syntax

seq *seq_num* { **match any** [[**source** *src_ip*] [**destination** *dst_ip*] | [**endpoint** *endpoint_ip*]] | [**type vxlan** [**vni** *value*]] }

no seq *seq_num*

no { **match any** [[**source** *src_ip*] [**destination** *dst_ip*] | [**endpoint** *endpoint_ip*]] | [**type vxlan** [**vni** *value*]] }

Command Default

No classification is applied.

Parameters

seq *seq_num*
Inserts a tunnel identifier in the class map at a certain position. Range is from 0 through 4294967290.

match any
Applies the specified flow filters to all active tunnels in the system.

source *src_ip* **destination** *dst_ip*
Specifies either the source, the destination, or both IP addresses as a tunnel identifier.

endpoint *endpoint_ip*
Specifies the IP address assigned to the tunneling endpoint within the system for filtering.

type vxlan
Specifies VXLAN tunnel type.

vni *value*
Specifies the VXLAN Network Identifier (VNI) to match against, and optionally also specify a VNI mask to use to filter a range of contiguous VNI values.

Modes

Overlay class map configuration mode

Usage Guidelines

Use the **no** forms of this command to delete the matching filter from the ACL..

A tunnel can be identified by the outer packet IP header. The user can specify either the source or the destination or both as a tunnel identifier. If both are not specified, an implicit "match any" is made for the missing option.

The user can specify the IP address assigned to the tunneling endpoint within the system for filtering. If the IP address of the specified endpoint occurs as either a source or a destination in the outbound packet, this is considered an overlay class map "hit."

Examples

The following example specifies a sequence number.

```
device# configure terminal
device(config)# overlay-class-map overlayclassmap1
device(config-overlay-classmap-overlayclassmap1)# seq 10
```

The following example applies the flow filter to all active tunnels in the system.

```
device# configure terminal
device(config)# overlay-class-map overlayclassmap1
device(config-overlay-classmap-overlayclassmap1)# seq 10 match any
```

History

Release version	Command history
17s.1.01	This command was introduced.

seq (rules in IPv4 extended ACLs)

Inserts filtering rules in IPv4 extended ACLs. Extended ACLs permit or deny traffic according to source and destination 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*]] { *D_IPaddress mask* | **host** *D_IPaddress* | **any** } [**dscp** *DSCPvalue*] [*destination-operator* [*D_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**log**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] { *D_IPaddress mask* | **host** *D_IPaddress* | **any** } [**dscp** *DSCPvalue*] [*destination-operator* [*D_port-numbers*]] [*TCP-flags*] [**count**] [**vlan** *vlanID*] [**log**]

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] { *D_IPaddress mask* | **host** *D_IPaddress* | **any** } [**dscp** *DSCPvalue*] [*destination-operator* [*D_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**log**]

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 and a sequence number is automatically assigned to it.

seq-value

Valid values range from 1 through 4294967290.

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

(Ignored for ACLs in overlay-transit policy maps) (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 and *destination-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

(Not supported for IPv4 ACLs in overlay-transit policy maps) 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

(Not supported for IPv4 ACLs in overlay-transit policy maps) 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

(Not supported for IPv4 ACLs in overlay-transit policy maps) The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

range

(Not supported for IPv4 ACLs in overlay-transit policy maps) 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 and *D_port_numbers*

(Valid only when *ip-protocol* is UDP or TCP) Specifies one or more source or destination port numbers.

D_IPaddress

Specifies a destination address for which you want to filter the sub-net.

mask

Defines a mask, whose effect is to specify a subnet that includes the destination address that you specified. For options to specify the mask, see the Usage Guidelines.

host
Specifies a destination address.

D_IPaddress
The destination address.

any
Specifies all destination addresses.

dscp
Matches *DSCPvalue* against the DSCP value of the packet.

DSCPvalue
From 0 through 63.

vlan *vlanID*
(Ignored for ACLs in overlay-transit policy maps) 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. If a rule that includes **count** is duplicated in both a security ACL and an overlay-gateway policy-map ACL, the counter is enabled only for the security ACL.

log
(Ignored for ACLs in overlay-transit policy maps) Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

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.

For ACLs in overlay-transit policy maps, the only mask supported is all bits set (indicating exact host match). So there is no advantage to defining a mask.

All parameters—including masks—are supported for ACLs in overlay-gateway policy maps. For IPv4 ACLs in overlay-transit policy maps, refer to the "Parameters" section.

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 for SLX 9140 and SLX 9240*.)

- 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.

All parameters are supported for ACLs in overlay-gateway policy maps. For IPv4 ACLs in overlay-transit policy maps, refer to the "Parameters" section.

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*.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified for support of Overlay Services.

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**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**]

no { **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**]

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 and a sequence number is automatically assigned to it.

seq-value

Valid values range from 1 through 4294967290.

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. If a rule that includes **count** is duplicated in both a security ACL and an overlay-gateway policy-map ACL, the counter is enabled only for the security ACL.

log

(Ignored for ACLs in overlay-transit policy maps) Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

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 logging.

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.

For ACLs in overlay-transit policy maps, the only mask supported is all bits set (indicating exact host match). So there is no advantage to defining a mask.

All parameters—including masks—are supported for ACLs in overlay-gateway policy maps. For IPv4 ACLs in overlay-transit policy maps, refer to the "Parameters" section.

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 for SLX 9140 and SLX 9240*.)

- 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
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified for support of Overlay Services.

seq (rules in IPv6 extended ACLs)

Inserts filtering rules in IPv6 extended ACLs. IPv6 extended ACLs permit or deny traffic according to source address, as well as other parameters.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] { **any** | *D_IPaddress* **/** *prefix_len* | **host** *D_IPaddress* } [*destination-operator* [*D_port-numbers*]] [**dscp** *DSCPvalue*] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] { **any** | *D_IPaddress* **/** *prefix_len* | **host** *D_IPaddress* } [*destination-operator* [*D_port-numbers*]] [**dscp** *DSCPvalue*] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**]

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] { **any** | *D_IPaddress* **/** *prefix_len* | **host** *D_IPaddress* } [*destination-operator* [*D_port-numbers*]] [**dscp** *DSCPvalue*]] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**]

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 4294967290.

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.

any
Specifies all destination addresses.

D_IPaddress
Specifies a destination 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 destination address.

D_IPaddress
The destination address. For options to abbreviate the address, see the Usage Guidelines.

destination-operator
Specifies one of the following destination operators:

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. The first port number in the range must be lower than the last number in the range.

D_port_numbers
(Valid only when *ip-protocol* is UDP or TCP) Specify one or more destination port numbers.

dscp
Matches *DSCPvalue* against the DSCP value of the packet.

DSCPvalue
From 0 through 63.

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.

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 at the end of the list and a sequence number is automatically assigned to it.

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 are not permitted.)

All parameters are supported for ACLs in overlay-gateway policy maps. Overlay-transit policy maps do not support MAC ACLs or IPv6 ACLs.

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*.

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-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)# hard-drop tcp host 10::3 host ff02::1 count
device(conf-ipacl-ext)# exit
device(config)# ipv6 receive access-group ipv6-receive-acl-example
```

History

Release version	Command history
17s.1.00	This command was introduced.

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**]

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**]

no { **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *SIP_address* | *SIP_addressmask* } [**count**] [**log**]

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 and a sequence number is automatically assigned to it.

seq-value

Valid values range from 1 through 4294967290.

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.

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 logging.

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 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 are not permitted.)

All parameters are supported for ACLs in overlay-gateway policy maps. Overlay-transit policy maps do not support MAC ACLs or IPv6 ACLs.

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 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

seq (rules in MAC extended ACLs)

Inserts filtering rules in a Layer 2 (MAC) extended ACLs. Extended ACLs permit or deny traffic according to source and destination addresses, as well as other parameters.

Syntax

[**seq** *seq-value*] { **deny** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [**vlan** { **all** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**count**] [**log**] [**mirror**]

seq *seq-value* { **permit** | **deny** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [*custom-EtherType* | **arp** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**vlan** *vlanID*] [**count**] [**log**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [*custom-EtherType* | **arp** | **ipv4** | **ipv6**] [**pcp** *pcp-match-value*] [**vlan** *vlanID*] [**count**] [**log**]

no permit { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [*custom-EtherType* | **arp** | **ipv4** | **ipv6**] [**vlan** *vlanID*] [**pcp** *pcp-match-value*] [**count**] [**log**]

no { **deny** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } { **any** | **host** *DMAC_address* | *DMAC_address mask* } [*custom-EtherType* | **arp** | **ipv4** | **ipv6**] [**vlan** *vlanID*] [**pcp** *pcp-match-value*] [**count**] [**log**]

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 and a sequence number is automatically assigned to it.

seq-value

Valid values range from 1 through 4294967290.

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 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.

any
Specifies all destination MAC addresses.

DMAC_address
Specifies a destination MAC address and a comparison mask.

mask
Specifies 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 destination MAC address.

DMAC_address
Use the format HHHH.HHHH.HHHH.

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.

ipv4
Specifies to permit or deny the IPv4 protocol (0x0800).

ipv6
Specifies to permit or deny the IPv6 protocol (0x86dd).

vlan *vlanID*
Specifies a VLAN interface to which the ACL is bound.

pcp *pcp-match-value*
Filters by PCP priority value. Permitted values are 0 through 7.

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.

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 and logging 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.

Although in an extended-ACL rule you can specify **mirror** and **log**, only one of the two is processed, as follows:

- In a permit rule, the order of precedence is **mirror** > **log**.
- In a deny or hard-drop rule, the order of precedence is **log** > **mirror**.

All parameters are supported for ACLs in overlay-gateway policy maps. Overlay-transit policy maps do not support MAC ACLs or IPv6 ACLs.

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 to enable the counting of packets.

```
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 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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**]

no seq *seq-value*

{ **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**]

no seq { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**]

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 and a sequence number is automatically assigned to it.

seq-value

Valid values range from 1 through 4294967290.

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 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.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source MAC address. You can also enable counters and logging.

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.

All parameters are supported for ACLs in overlay-gateway policy maps. Overlay-transit policy maps do not support MAC ACLs or IPv6 ACLs.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

seq overlay-class

Creates a stanza within an overlay policy and defines the classification method to be used to identify the desired tunnel.

Syntax

seq *seq_num* **overlay-class** *name*

no seq *seq_num*

Command Default

No stanza is created.

Parameters

seq *seq_num*

Inserts a new stanza and classification within the overlay policy map. Range is from 0 through 4294967290.

name

Identifies the tunnel on which to perform specific actions or flows.

Modes

Overlay policy map configuration mode

Usage Guidelines

If a sequence value is not specified, the defined stanza is assigned the next highest available sequence value.

The overlay class map name must already exist and be provisioned, or else an error is returned.

Use the **no** form of this command to delete the matching stanza from the policy. To delete the stanza and all associated flows and actions, the user must simply use the **no** form. The classification map name is not required, because a stanza can include only one overlay class map directive.

Examples

The following example inserts a new stanza and classification within an overlay policy map.

```
device# configure terminal
device(config)# overlay-policy-map overlaypolicymap1
device(config-overlay-policymap)# seq 10 overlay-class overlayclass1
```

The following example deletes the matching stanza from the policy.

```
device# configure terminal
device(config)# overlay-policy-map overlaypolicymap1
device(config-overlay-policymap)# no seq 10
```

History

Release version	Command history
17s.1.01	This command was introduced.

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 7**.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

service-policy

Binds a policy map to inbound traffic on an interface.

Syntax

service-policy *policy-mapname*

no service-policy *policy-mapname*

Command Default

No service policy is created.

Parameters

in
Binds the policy map to inbound traffic.

out
Binds the policy map to outbound traffic.

policy-mapname
Name of the policy map.

Modes

Interface configuration mode

Usage Guidelines

This command applies a policy-map containing a class-map with specific policer parameters and match criteria to a switch 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

The following binds a service policy for inbound traffic on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/8
device(conf-if-eth-0/8)# service-policy in policymap1
```

The following removes a service policy for inbound traffic from a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/8
device(conf-if-eth-0/8)# no service-policy policymap1
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified.

set (policer)

Establishes a new setting in the default policer remark profile for the specified remark values.

Syntax

set *remark-value value-setting*

Command Default

The **police-remark-profile** command has been executed. Then, the **action** command has been executed, specifying the **color** classification type.

Parameters

remark-value
Specifies which remark value is to be modified.

value-setting
Specifies the value to be set for the specified remark value.

Modes

Policer remarking profile configuration mode

Usage Guidelines

Use this command after executing the **police-remark-profile** command and after executing the **action** command, specifying **color** as the classification type. You issue the **set** command to specify remark values in the default policer remark profile for **cos**, **traffic-class**, and **dscp**.

Examples

The following is an example of executing the **set** command to specify the settings in the default policer remark profile for the remark values for conforming traffic.

```
device# configure terminal
device(config)# police-remark-profile default
device(police-remark-profile-default)# action color conform
device(police-remark-profile-color-conform)# set cos 3
device(police-remark-profile-color-conform)# set traffic-class 5
device(police-remark-profile-color-conform)# set dscp 10
device(police-remark-profile-color-conform)# exit
```

History

Release version	Command history
17s.1.00	This command was introduced.

set as-path

Sets a prepended string or a tag for an AS-path attribute in a route-map instance.

Syntax

set as-path { **prepend** *string* | **tag** }

no set as-path { **prepend** *string* | **tag** }

Parameters

prepend

Prepends the string to the AS-path.

string

AS numbers. Range is from 1 through 4294967295.

tag

Converts the tag of a route into an autonomous system path.

Modes

Route-map configuration mode

Examples

The following example a prepended string or a tag for an AS-path attribute in a route-map instance.

```
device# configure terminal
device(config)# routemap myroutemap1 permit 10
device(config-route-map-myroutemap1/permit/10)# set as-path prepend 7701000
```

History

Release version	Command history
17s.1.00	This command was introduced.

set automatic-tag

Sets the route-map tag value.

Syntax

set automatic-tag *value*

Parameters

value

The value for the computed tag.

Modes

Global configuration mode

Examples

The following example sets a route-map tag value of 5.

```
device# configure terminal
device(config)# route-map myroutemap permit 10
device(config-route-map myroutemap/permit/10)# set automatic-tag 5
```

History

Release version	Command history
17s.1.00	This command was introduced.

set comm-list

Sets a community list for deletion in a route-map instance.

Syntax

set comm-list *name*

no set comm-list *name*

Parameters

name

Community list name. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** version of this command to disable this feature.

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 comm-list test
```

History

Release version	Command history
17s.1.00	This command was introduced.

set community

Sets a BGP community attribute in a route-map instance.

Syntax

set community [*community-number* | additive | internet | local-as | no-advertise | no-export | none]

no set community *community-number*

Parameters

community-number
BGP community number, in two format options:(1) Range is from 1 through 4294967295.(2) Format is AA:NN, where AA is the AS number, and NN is a locally significant number.

additive
Add to the existing community.

internet
Send to internet (well-known community).

local-as
Do not send outside local AS (well-known community).

no-advertise
Do not advertise to any peer (well-known community).

no-export
Do not export to next AS (well-known community).

none
Sets no community attribute.

Modes

Route-map configuration mode

Examples

The following example sets a BGP community attribute that does not export to the next AS in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set community no-export
```

History

Release version	Command history
17s.1.00	This command was introduced.

set dampening

Sets a BGP route-flap dampening penalty in a route-map instance.

Syntax

set dampening { **half-life** *number* | **reuse** *number* | **suppress***number* | **max-suppression***number* }

no set dampening *number*

Command Default

The default is 15.

Parameters

half-life *number*
Half-life in minutes for the penalty. Range is from 1 through 45.

reuse *number*
Route that is unsuppressed if the penalty for a flapping route decreases enough to fall below this value. The process of unsuppressing routes occurs at 10-second increments. Range is from 1 through 20000.

suppress *number*
Value at which to start suppressing a route. Range is from 1 through 20000.

max-suppression *number*
Maximum duration in minutes to suppress a stable route. Range is from 1 through 255.

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of the command removes the penalty.

Examples

The following example sets a maximum duration of 25 minutes for a BGP route-flap dampening penalty in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set dampening 25
```

History

Release version	Command history
17s.1.00	This command was introduced.

set distance

Sets the administrative distance for matching OSPF routes in route-map instance.

Syntax

set distance *value*

no set distance

Parameters

value

Administrative distance for the route. Range is from 1 through 254.

Modes

Route-map configuration mode

Usage Guidelines

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

Examples

The following example sets an administrative distance of 50 for matching OSPF routes in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set distance 50
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The **no** form of the command deletes 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

set interface (NPB route-maps)

Specifies an egress interface for a route-map used to implement Network Packet Broker (NPB) policy.

Syntax

[**precedence** *precedence-value*] **set interface** { **ethernet** *slot* **/** *port* | **port-channel** *number* | **pbf-destination-group** *pbf-dest-group-id* } [**strip-vlan outer**] [**add-vlan outer** *vlan-id*]

no precedence *precedence-value*

no set interface { **ethernet** *slot* **/** *port* | **port-channel** *number* | **pbf-destination-group** *pbf-dest-group-id* } [**strip-vlan outer**] [**add-vlan outer** *vlan-id*]

Parameters

precedence

(Optional) Enables you to assign a precedence number to the set statement. If you do not specify **precedence** *precedence-value*, the statement is added at the end of the route map and a precedence number is automatically assigned to it.

precedence-value

Values range from 1 through 65535.

ethernet *slot* **/** *port*

Specifies an Ethernet interface. The slot number must be 0 if the switch does not contain slots.

null0

(Not implemented under NPB) Specifies the Null0 interface, dropping the packet.

port-channel *number*

Specifies a port-channel interface.

pbf-destination-group *pbf-dest-group-id*

Specifies a policy-based forwarding (PBF) destination-group ID. Values range from 1 through 8192.

strip-vlan outer

Removes outer VLAN headers from the egressing packet.

add-vlan outer *vlan-id*

Adds an outer C-VLAN tag, specifying a VLAN ID. VLAN IDs range from 1 through 4090.

Modes

Route-map configuration mode

Usage Guidelines

This command is supported only under NPB system mode. If the system mode is default, set it to NPB, using the **system-mode** command.

The order of the set statements in a route-map is critical: In general, a match followed by a valid **set interface** or **set next-hop-tvf-domain** statement stops further processing. Specifying precedence values determines the order of statement processing. If

you do not specify precedence values, they are automatically assigned as follows: The first set statement is assigned "precedence 10", the second is assigned "precedence 20", and so forth.

To display policy-map set-statement precedence values, run the **show running-config route-map** command. The results will make it easier for you to add additional set statements in the required order.

Adding a VLAN tag enables you to mark network traffic for custom processing downstream, such as application-specific filtering on an interconnected packet broker or special handling by the analytics application.

You cannot have both **set interface** {**ethernet** | **port-channel** } and **set interface pbf-destination-group** commands in a stanza.

To delete a **set interface** statement from a route map, perform one of the following actions:

- If you know the precedence number, enter **no precedence** *precedence-value*.
- If you do not know the precedence number, type **no** followed by the full syntax without **precedence** *precedence-value*.

Examples

The following example configures ingress traffic from Ethernet 0/1 and port-channel 100 to egress Ethernet 0/5.

```
device# configure terminal
device(config)# route-map npb_map permit 10
device(config-route-map-npb_map/permit/10)# set interface ethernet 0/5
device(config-route-map-npb_map/permit/10)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# npb policy route-map npb_map
device(conf-if-eth-0/1)# exit
device(config)# interface port-channel 100
device(config-Port-channel-100)# npb policy route-map npb_map
```

The following NPB-grid example creates destination 5 within destination group 99. It then configures ingress traffic from Ethernet 0/1 and port-channel 100 to destination group 99.

```
device# configure terminal
device(config)# pbf destination 5
device(config-destination-5)# statistics-enable
device(config-destination-5)# precedence 10 set interface eth 0/12:3
device(config-destination-5)# exit
device(config)# pbf destination-group 99
device(config-destination-group-99)# add destination 5
device(config-destination-group-99)# exit

device(config)# route-map npb_map permit 10
device(config-route-map-npb_map/permit/10)# set interface pbf-destination-group 99
device(config-route-map-npb_map/permit/10)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# npb policy route-map npb_map
device(conf-if-eth-0/1)# exit
device(config)# interface port-channel 100
device(config-Port-channel-100)# npb policy route-map npb_map
```

History

Release version	Command history
17s.1.01	This command was introduced.
18s.1.00	This command was modifed to support the **add-vlan outer** *vlan-id* option.
18s.1.02	This command was modifed to support the **pbf-destination-group** option.

set interface (PBF destination)

In a policy-based forwarding (PBF) destination, specifies a physical or port-channel interface for forwarding traffic.

Syntax

[**precedence** *precedence-value*] **set interface** { **ethernet** *slot* **/** *port* | **port-channel** *number* } [**type-fabric**]

no precedence *precedence-value* **set interface**

no set interface { **ethernet** *slot* **/** *port* | **port-channel** *number* } [**type-fabric**]

Parameters

precedence

(Optional) Enables you to assign a precedence number to the set statement. If you do not specify **precedence** *precedence-value*, the statement is added at the end of the route map and a precedence number is automatically assigned to it.

precedence-value

Values range from 1 through 65535.

ethernet *slot* **/** *port*

Specifies an Ethernet interface. The slot number must be 0 if the switch does not contain slots.

port-channel *number*

Specifies a port-channel interface.

type-fabric

For an edge destination, do not specify this keyword. Not specifying **type-fabric** strips the internal encapsulation and presents the original frame to the end user. You typically include the **type-fabric** keyword for traffic destined to a distributor.

Modes

PBF-destination configuration mode

Usage Guidelines

This use-case for this command is under NPB system mode. If the system mode is default, set it to NPB, using the **system-mode** command.

The set statement with the smallest precedence number is the preferred path to the destination and is selected if available. The next set statement becomes active only if the preferred destination is down. If the preferred destination recovers, it again becomes the active path.

To delete a **set interface** statement from a destination, perform one of the following actions:

- If you know the precedence number, enter **no precedence** *precedence-value*.
- If you do not know the precedence number, type **no** followed by the full syntax without **precedence** *precedence-value*.

Examples

The following example configures "edge" interfaces for a PBF destination.

```
device# configure terminal
device(config)# pbf destination 10
device(config-destination-10)# precedence 10 set interface ethernet 0/1
device(config-destination-10)# precedence 20 set interface ethernet 0/2
device(config-destination-10)# precedence 40 set interface port-channel 5
```

The following example configures "fabric" interfaces for a PBF destination.

```
device# configure terminal
device(config)#  pbf destination 20
device(config-destination-20)# set interface eth 0/4  type-fabric
device(config-destination-20)# set interface eth 0/3  type-fabric
```

History

Release version	Command history
18s.1.02	This command was introduced.

set local-preference

Specifies a preference value for the autonomous system path.

Syntax

set local-preference *number*

no set local-preference

Parameters

number

The route distance value range is from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of the command removes the attribute.

Examples

The following example specifies a preference value of 8675309 for the autonomous system path.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)#  set local-preference 8675309
```

History

Release version	Command history
17s.1.00	This command was introduced.

set metric

Configures the route metric set clause in a route-map instance.

Syntax

set metric { **add** | **assign** | **sub** } *value*

set metric none

no set metric { **add** | **assign** | **sub** } *value*

no set metric none

Parameters

add
Adds the value to the current route metric.

assign
Replaces the current route metric with this value.

sub
Subtracts the value from the current route metric.

value
Specifies a value. Valid values range from 0 through 4294967295.

none
Removes the current route metric.

Modes

Route-map configuration mode

Examples

The following example adds a value of 256 to the current route metric in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutemap/permit/10)# set metric add 256
```

History

Release version	Command history
17s.1.00	This command was introduced.

set metric-type

Sets a variety of metric types for destination routing in a route-map instance.

Syntax

set metric-type [*type-1* | *type-2*]

no set metric-type [*type-1* | *type-2*]

Parameters

type-1
OSPF external type-1 metric

type-2
OSPF external type-2 metric

Modes

Route-map configuration mode

Usage Guidelines

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

Examples

The following example sets a variety of metric types for destination routing in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set metric-type type-1
```

History

Release version	Command history
17s.1.00	This command was introduced.

set next-hop-tvf-domain

Specifies a Transparent VLAN Flooding (TVF) domain as the next hop for a Network Packet Broker (NPB) route map to support replication of traffic to multiple interfaces.

Syntax

[**precedence** *precedence-value*] **set next-hop-tvf-domain** *tvf-domain-ID* [**strip-vlan outer**] [**add-vlan outer** *vlan-id*]

no precedence *precedence-value*

no set next-hop-tvf-domain *tvf-domain-ID* [**strip-vlan outer**] [**add-vlan outer** *vlan-id*]

Command Default

TVF domain as the route map next hop is not configured.

Parameters

precedence

(Optional) Enables you to assign a precedence number to the set statement. If you do not specify **precedence** *precedence-value*, the statement is added at the end of the route map and a precedence number is automatically assigned to it.

precedence-value

Values range from 1 through 65535.

tvf-domain-ID

Specifies the ID of the TVF domain. Values are from 1 through 4096.

strip-vlan outer

Removes outer VLAN headers from the egressing packet.

add-vlan outer *vlan-id*

Adds an outer C-VLAN tag, specifying a VLAN ID. VLAN IDs range from 1 through 4090.

Modes

Route map configuration mode

Usage Guidelines

This command is supported only under NPB system mode. If the system mode is default, set it to NPB, using the **system-mode** command.

For load-balanced output when flooding, make sure that the TVF domain includes a port-channel.

The order of the set statements in a route-map is critical: In general, a match followed by a valid **set interface** or **set next-hop-tvf-domain** statement stops further processing. Specifying precedence values determines the order of statement processing. If you do not specify precedence values, they are automatically assigned as follows: The first set statement is assigned "precedence 10", the second is assigned "precedence 20", and so forth.

To display policy-map set-statement precedence values, run the **show running-config route-map** command. The results will make it easier for you to add additional set statements in the needed order.

To delete a **set next-hop-tvf-domain** statement from a route map, perform one of the following actions:

- If you know the precedence number, enter **no precedence** *precedence-value*.
- If you do not know the precedence number, type **no** followed by the full syntax without **precedence** *precedence-value*.

Examples

The following example configures—in a route map—a specified TVF domain as the next hop.

```
device# configure terminal
device(config)# route-map TVFtest permit 99
device(config-route-map-TVFtest/permit/99)# set next-hop-tvf-domain 5
```

History

Release version	Command history
17s.1.01	This command was introduced.
18s.1.00	This command was modifed to support the **add-vlan outer** *vlan-id* option.

set origin

Sets a BGP origin code in a route-map instance.

Syntax

set origin [*igp* | *incomplete*]

no set origin [*igp* | *incomplete*]

Parameters

igp
Local IGP

incomplete
Unknown heritage

Modes

Route-map configuration mode

Usage Guidelines

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

Examples

The following example sets a BGP origin code in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set origin incomplete
```

History

Release version	Command history
17s.1.00	This command was introduced.

set tag

Sets the route tag value in a route-map instance.

Syntax

set tag *value*

no set tag *value*

Parameters

value

The tag clause value for the route-map. Range is from 0 through 4294967295.

Modes

Privileged EXEC mode

Usage Guidelines

The **no** form of this command disables this feature.

Examples

The following example sets a route tag value in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set tag 8675309
```

History

Release version	Command history
17s.1.00	This command was introduced.

set weight

Sets a BGP weight for the routing table in a route-map instance.

Syntax

set weight *number*

no set weight *number*

Parameters

number

Specifies a weight value. Valid values range 0 through 65535.

Modes

Route-map configuration mode

Examples

The following example sets a BGP weight for the routing table in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set weight 500
```

History

Release version	Command history
17s.1.00	This command was introduced.

sflow collector

Configures the forwarding of sFLow datagrams to collectors.

Syntax

sflow collector { *IPv4address* | *IPv6address* } { *port_num* } [**use-vrf** *vrf-name*]

no sflow collector { *IPv4address* | *IPv6address* } [*port_num*] [**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.

port_num
Specifies the port number to use for sendng data to the collector. Range is 1 through 65535. The default is 6343.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

sflow enable (global version)

Enables sFlow globally.

Syntax

sflow enable

no sflow enable

Command Default

sFlow is disabled on the system.

Modes

Global configuration mode

Usage Guidelines

This command is supported on physical ports only.

The **no** form of this command disable sFlow globally.

Examples

To enable sFlow globally:

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

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

sflow sample-rate (global version)

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 global default sampling rate: 2048 packets.

Parameters

samplerate

Specifies the sampling rate value in packets. Valid values range from 2 to 1044480 packets.

Modes

Global configuration mode

Usage Guidelines

Sample-rate is the average number of packets skipped before the sample is taken.

The **no** form of this command restores the default sampling rate.

Examples

To change the sampling rate to 4096:

```
device# configure terminal
device(config)# sflow sample-rate 4096
```

History

Release version	Command history
17s.1.00	This command was introduced.

sflow source-interface

Specifies the IPv4 or IPv6 address of either the Ethernet, Virtual Ethernet (ve), or loopback interface as the source of sFlow packets.

Syntax

sflow source-interface { **ethernet** *slot/port* | **loopback** *loopback_num* | **ve** *ve_interface* }

no sflow source-interface

Command Default

sFlow uses the ethernet port by default.

Parameters

ethernet *slot/port*
Specifies an Ethernet slot and port. The valid slot value is 0.

loopback *loopback_num*
Specifies a loopback interface. Valid values range from 1 through 255.

ve *ve-interface-number*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 255.

Modes

Global configuration mode

Usage Guidelines

The "no" form of the command is available once the source type has been specified.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

shape

Specifies the shaping rate for a port to smooth out the traffic egressing an interface

Syntax

shape *speed*

Parameters

speed

The speed for the shape rate in Kbps. Range is from 50000 through 100000000 Kbps.

Modes

Policymap configuration mode

Usage Guidelines

This command is allowed only for the egress direction.

This command can only be configured for the "default" class.

This command is mutually exclusive with respect to the **scheduler** and **police** commands.

Examples

The following example sets a shape-rate speed of 50000 Kbps.

```
device# configure terminal
device(config)# policy-map mypolicymap
device(config-policymap)# class default
device(config-policymap-class)# shape 500000
```

History

Release version	Command history
17s.1.01	This command was introduced.

Show A through Show I

show access-list

Displays ACL status information for a given network, protocol, and inbound/outbound direction.

Syntax

The following statement displays a summary of ACL statuses on the device:
show access-list { **ip** | **ipv6** | **mac** }

The following statement displays the status of an ACL on all device interfaces—applied to incoming or outgoing traffic:
show access-list { **ip** | **ipv6** | **mac** } *name* { **in** | **out** }

The following statements display the statuses on an interface of all ACLs applied to incoming or outgoing traffic:
show access-list interface { **ethernet** *slot* **/** *port* | **management** *port* | **port-channel** *index* } **in**

show access-list { **ve** *vlan_id* | **vlan** *vlan_id* } { **in** | **out** }

The following statements display the rules in an ACL applied to incoming or outgoing traffic on an interface:
show access-list mac *name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* } **in**

show access-list mac *name* **interface vlan** *vlan_id* { **in** | **out** }

show access-list { **ip** | **ipv6** } *name* **interface** { **ethernet** *slot* **/** *port* | **management** *port* | **port-channel** *index* } **in**

show access-list { **ip** | **ipv6** } *name* **interface ve** *vlan_id* { **in** | **out** }

The following statement displays the status of all receive ACLs (rACLs) applied to the device:
show access-list global in

The following statement displays details of a specified rACL applied to the device:
show access-list { **ip** | **ipv6** } *name* **global in**

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 incoming binding direction.

out
: Specifies outgoing binding direction.

name
: Specifies the ACL name.

interface
Filters by interface.

ethernet
Specifies a physical 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 *index*
Specifies a port-channel interface.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

vlan *vlan_id*
Specifies a VLAN interface.

management *port*
Specifies a management interface.

global
Specifies Level 3 receive ACLs (rACLs), which are applied at device-level, rather than at interface-level.

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.

Command 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.
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 0/2
   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 0/4 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 0/4 in
ipv6 access-list ipv6-std-acl on Ethernet 0/4 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
ipv4 access-list extended ipv6-receive-acl-example
    seq 76 deny ip 10.10.95.10 0.0.0.0 any count (Active)

ipv6 access-list extended ipv6-receive-acl-example
    seq 10 deny ipv6 3001:2010:145:35::/64 any count (Active)
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

port-channel *index*
Specifies a port-channel interface.

Modes

Privileged EXEC mode

Command 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
-------------------------------------------------------------------------
```

History

Release version	Command history
17s.1.00	This command was introduced.

show access-list-log buffer config

Displays the configuration of the ACL buffer.

Syntax

show access-list-log buffer config

Modes

Privileged EXEC mode

Command 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 0/11
Buffer type is Circular and size is 512
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

ve *ve_id*
Specifies a virtual Ethernet (VE) interface.

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

Command 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".
Interface	Displays the physical or VE interface.

Output field	Description
MacResolved	Indicates if the record is listed in the MAC-address table. For a physical interface, displays "yes." For a VE, displays "yes" or "no".
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 "Dynamic", "Static", or "PreArp". ("PreArp" is ARP triggered other than by the data traffic, for example, by the static route.)

Examples

The following example displays the output of the basic **show arp** command.

```
device# show arp
Address          Mac-address     Interface     MacResolved   Age          Type
-------------------------------------------------------------------------------
11.1.1.20        UnResolved      Eth 0/14      yes           00:00:00     PreArp
12.1.1.20        UnResolved      Ve 10         no            00:00:00     PreArp
11.1.1.111       0610.9427.a001  Eth 0/14      yes           00:01:27     Dynamic
12.1.1.111       0410.9428.0002  Ve 10         yes           00:01:21     Dynamic
11.1.1.141       0000.0011.0141  Eth 0/14      yes           Never        Static
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
     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
     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
     permit ip host 30.30.30.1 mac host 0011.9400.0002
```

History

Release version	Command history
17s.1.00	This command was introduced.

show bfd

Displays Bidirectional Forwarding Detection (BFD) information.

Syntax

show bfd

Modes

Privileged EXEC mode

Command 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.
All Sessions	
Current	The number of BFD sessions currently 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 will be displayed only if it has at least one session on that interface.
MinTx	The interval in milliseconds between which the device desires to send a BFD message from this port to its peer.
MinRx	The interval in milliseconds that this device desires to receive a BFD message from its peer on this port.
Mult	The number of times that the device will wait for the MinRx time on this port before it determines that its peer device is nonoperational.
Sessions	The number of BFD sessions originating on this port.

Examples

The following example shows sample output from the **show bfd** command.

```
device# show bfd

  BFD State: ENABLED, Version: 1
  Supported Protocols: bgp, static-ip, tunnel, ospf, ospf6
  All Sessions: Current: 72 Max Allowed: 250 Max Exceeded Count: 0

  Port            MinTx       MinRx       Mult Sessions
  ====            =====       =====       ==== ========
  Eth 0/51        500         500         3    1
  Eth 0/54        500         500         3    1
  Ve 3001         500         500         3    2
  Ve 3009         500         500         3    2
  Ve 3011         500         500         3    2
  Ve 3019         500         500         3    2
  Ve 3021         500         500         3    2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command Output

The **show bfd neighbors** command displays the following information:

Output field	Description
OurAddr	Specifies the source IPv4 and IPv6 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

OurAddr                                 NeighAddr                               State     Int
=======                                 =========                               =====     ===
118.113.0.0                             118.113.0.1                             DOWN      Eth 0/54
113.113.113.113                         118.118.118.118                         UP        Lo 1
```

The following example shows sample output from the **show bfd neighbors** command when the **vrf** keyword is used.

```
device# show bfd neighbors vrf v3001

OurAddr                                 NeighAddr                               State     Int
=======                                 =========                               =====     ===
fe80::629c:9fff:fe5b:601                fe80::629c:9fff:fe87:3601               UP        Ve 3001
30.1.1.3                                30.1.1.8                                UP        Ve 3001
30.9.1.3                                30.9.1.8                                UP        Ve 3009
fdcd:3001:3009:1::113                   fdcd:3001:3009:1::118                   UP        Ve 3009
```

The following example shows sample output from the **show bfd neighbors** command when the **vrf** and **details** keywords are used.

```
device# show bfd neighbors vrf v3001 details

OurAddr                                 NeighAddr                               State     Int
=======                                 =========                               =====     ===
fe80::629c:9fff:fe5b:601                fe80::629c:9fff:fe87:3601               UP        Ve 3001

  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): 500    MinRxInt(ms): 500    Multiplier: 3
  Received MinTxInt(ms): 500    MinRxInt(ms): 500    Multiplier: 3
  Rx Count: 401700              Tx Count: 345604
  LD/RD:         80/172         Heard from Remote: Y
  Current Registered Protocols: ospf6
  Uptime: 1 day 19 hour 23 min 38 sec 78 msec
```

History

Release version	Command history
17s.1.00	This command was introduced.

show bfd neighbors application

Displays Bidirectional Forwarding Detection (BFD) neighbor session information.

Syntax

show bfd neighbors application { **bgp** | **ospf** | **ospf6** | **static-ip** | **tunnel** [**details**] }

Parameters

bgp
Specifies Border Gateway Protocol (BGP) sessions.

ospf
Specifies Open Shortest Path First (OSPF) sessions.

ospf6
Specifies Open Shortest Path First version 3 (OSPFv3) sessions.

static-ip
Specifies IP static route sessions.

tunnel
Specifies a tunnel interface.

details
Displays detailed neighbor session information.

Modes

Privileged EXEC mode

Command 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.
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 application** command when the **ospf** keyword is used.

```
device# show bfd neighbors application ospf

OurAddr                                 NeighAddr                               State     Int
=======                                 =========                               =====     ===
31.51.151.3                             31.51.151.8                             UP        Ve 3151
31.31.131.3                             31.31.131.8                             UP        Ve 3131
31.21.121.3                             31.21.121.8                             UP        Ve 3121
```

The following example shows sample output from the **show bfd neighbors application** command when the **ospf** and **details** keywords are used.

```
device# show bfd neighbors application ospf details

OurAddr                                 NeighAddr                               State     Int
=======                                 =========                               =====     ===
31.81.181.3                             31.81.181.8                             UP        Ve 3181

  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): 500    MinRxInt(ms): 500    Multiplier: 3
  Received MinTxInt(ms): 500    MinRxInt(ms): 500    Multiplier: 3
  Rx Count: 127097              Tx Count: 142393
  LD/RD:          3/81          Heard from Remote: Y
  Current Registered Protocols: ospf
  Uptime: 0 day 15 hour 53 min 12 sec 939 msec
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **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. The slot number specified must be 0 if the switch does not contain slots.

loopback *number*
Specifies a loopback interface. Valid values range from 1 through 255.

ve *ve-interface-number*
Specifies a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Command 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.

Output field	Description
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.

```
device# show bfd neighbors dest-ip 118.118.118.118

OurAddr                                 NeighAddr                                 State     Int
=======                                 =========                                 =====     ===
113.113.113.113                         118.118.118.118                           UP        Lo 1
```

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 118.118.118.118 details

OurAddr                                 NeighAddr                                 State     Int
=======                                 =========                                 =====     ===
113.113.113.113                         118.118.118.118                           UP        Lo 1

  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): 500    MinRxInt(ms): 500    Multiplier: 3
  Received MinTxInt(ms): 500    MinRxInt(ms): 500    Multiplier: 3
  Rx Count: 941487              Tx Count: 1016042
  LD/RD:          2/69          Heard from Remote: Y
  Current Registered Protocols: static-ip
  Uptime: 0 day 15 hour 54 min 20 sec 683 msec
```

History

Release version	Command history
17s.1.00	This command was introduced.

show bfd neighbors details

Displays detailed Bidirectional Forwarding Detection (BFD) neighbor information.

Syntax

show bfd neighbors details

Modes

User EXEC mode

Command Output

The **show bfd neighbors details** command displays the following information:

Output field	Description
OurAddr	Specifies the source IPv4 and IPv6 address of the interface on which this BFD session is running.
NeighAddr	Specifies the IPv4 or IPv6 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.
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

Output field	Description
MinTxInt(ms)	The interval in milliseconds between which the device will send a BFD message from this local neighbor port to its peer.
MinRxIntMinTxInt(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	
MinTxInt(ms)	The interval in milliseconds between which the peer device will send a BFD message from the remote neighbor port to its peer.
MinRxIntMinTxInt(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 descriptor
Heard from Remote	Indicates remote BFD neighbor has been heard.
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.

Examples

The following example shows sample output from the **show bfd neighbors details** command.

```
device# show bfd neighbors details

OurAddr                                 NeighAddr                                State     Int
=======                                 =========                                =====     ===
118.113.0.0                             118.113.0.1                              DOWN      Eth 0/54

  Local    State: DOWN          Diag: 0             Demand mode: 0    Poll: 0
  Received State: A.DOWN        Diag: 0             Demand mode: 0    Poll: 0    Final: 0
  Local    MinTxInt(ms): 500    MinRxInt(ms): 500   Multiplier: 3
  Received MinTxInt(ms): 0      MinRxInt(ms): 0     Multiplier: 0
  Rx Count: 0                   Tx Count: 230955
  LD/RD:          1/0           Heard from Remote: N
  Current Registered Protocols: bgp, static-ip
  Uptime: 0 day 0 hour 0 min 0 sec 0 msec

OurAddr                                 NeighAddr                                State     Int
=======                                 =========                                =====     ===
113.113.113.113                         118.118.118.118                          UP        Lo 1

  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): 500    MinRxInt(ms): 500   Multiplier: 3
  Received MinTxInt(ms): 500    MinRxInt(ms): 500   Multiplier: 3
  Rx Count: 474365              Tx Count: 490778
  LD/RD:          2/69          Heard from Remote: Y
  Current Registered Protocols: static-ip
  Uptime: 1 day 19 hour 26 min 47 sec 197 msec
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **ve** *ve-interface-number* } [**details**]

Parameters

ethernet *slot/port*
Specifies an Ethernet slot and port. The slot number specified must be 0 if the switch does not contain slots.

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.

ve *ve-interface-number*
Specifies a virtual Ethernet (VE) interface.

details
Specifies detailed information.

Modes

Privileged EXEC mode

Command 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.
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 interface** command when the **ve** and **details** keywords are used.

```
device# show bfd neighbors interface ve 3109 details

OurAddr                                 NeighAddr                                 State     Int
=======                                 =========                                 =====     ===
31.9.101.3                              31.9.101.8                                UP        Ve 3109

  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): 500    MinRxInt(ms): 500    Multiplier: 3
  Received MinTxInt(ms): 500    MinRxInt(ms): 500    Multiplier: 3
  Rx Count: 347776              Tx Count: 389488
  LD/RD:        122/197         Heard from Remote: Y
  Current Registered Protocols: bgp
  Uptime: 1 day 19 hour 28 min 19 sec 509 msec
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.01	This command was introduced.

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*] | *type*]

Parameters

ip-addr
Specifies the IPv4 address of a neighbor.

ipv6-addr
Specifies the IPv6 address of a neighbor.

detail *type*
Specifies detailed information be given for the designated route type.

type
Specifies the type of route.

arp
Specifies Address Resolution Protocol (ARP) routes.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segment (ES) 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 (ND) 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 2.0.0.2 advertised-routes detail

       There are 5812 routes advertised to neighbor 2.0.0.2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
1       Prefix: ARP:[0][0000.abba.baba]:[IPv4:2.29.1.254],  Status: BE,  Age: 1d6h1m40s
         NEXT_HOP: 19.0.0.19, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            Extended Community: ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT
65003:29 RT 2:2 RT 65003:20 ExtCom:06:03:50:eb:1a:13:17:9a
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 29 L3_vni: 20 Router Mac : 50:eb:1a:13:17:9a
            ESI : 00.0000000000000000000
2       Prefix: ND:[0][0000.abba.abba]:[IPv6:2:29:1::254],  Status: BE,  Age: 1d6h1m40s
         NEXT_HOP: 19.0.0.19, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            Extended Community: ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT
65003:29 RT 2:2 RT 65003:20 ExtCom:06:03:50:eb:1a:13:17:9a
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 29 L3_vni: 20 Router Mac : 50:eb:1a:13:17:9a
            ESI : 00.0000000000000000000
3       Prefix: MAC:[0][50eb.1a13.8074],  Status: BE,  Age: 1d6h1m35s
         NEXT_HOP: 76.0.0.76, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            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 65003:136
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 136
            ESI : 00.0000000000000000000
4       Prefix: MAC:[0][0000.abba.baba],  Status: BE,  Age: 1d6h1m35s
         NEXT_HOP: 76.0.0.76, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            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 65003:136
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 136
            ESI : 00.0000000000000000000
5       Prefix: MAC:[0][0000.abba.abba],  Status: BE,  Age: 1d6h1m35s
         NEXT_HOP: 76.0.0.76, Learned from Peer: 200.1.1.76 (65003)
          LOCAL_PREF: none,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 65009 65003
            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 65003:136
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 2,  Admin distance 20
            L2_vni: 136
            ESI : 00.0000000000000000000
…
```

History

Release version	Command history
17r.1.01	This command was introduced.

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.

arp
Specifies Address Resolution Protocol (ARP) routes.

auto-discovery
Specifies automatically discovered routes.

ethernet-segment
Specifies Ethernet Segments (ES) routes.

inclusive-multicast
Specifies inclusive multicast routes.

mac
Specifies MAC routes.

nd
Specifies neighbor discovery (ND) 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 2.0.0.2 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][IPv4:57.0.0.57]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
         L2_vni: 22
2      ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 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      BE
         AS_PATH: 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      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
5      MAC:[0][0000.abba.abba]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
…
```

The following example shows output for the **show bgp evpn neighbors routes best** command when the **nd** keyword is used.

```
device# show bgp evpn neighbors 2.0.0.2 routes best type nd

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      ND:[0][0000.abba.abba]:[IPv6:2:22:1::254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
2      ND:[0][0027.f8ca.76ba]:[IPv6:fe80::227:f8ff:feca:76ba]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
3      ND:[0][0000.abba.abba]:[IPv6:2:23:1::254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 23 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      BE
         AS_PATH: 65002 65006
            L2_vni: 23 L3_vni: 0
         ESI : 00.000000000000000000
5      ND:[0][0000.abba.abba]:[IPv6:2:24:1::254]
                           57.0.0.57        0          100        0      BE
         AS_PATH: 65002 65006
            L2_vni: 24 L3_vni: 0
         ESI : 00.000000000000000000
…
```

History

Release version	Command history
17s.1.01	This command was introduced.

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      ?
```

History

Release version	Command history
17s.1.01	This command was introduced.

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:
```

History

Release version	Command history
18s.1.01	This command was introduced.

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:
```

History

Release version	Command history
18s.1.01	This command was introduced.

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
```

History

Release version	Command history
17s.1.01	This command was introduced.

show bridge-domain

Displays information about the bridge domains.

Syntax

show bridge-domain [*id* [**logical-interface**]]

show bridge-domain brief [{ **p2mp** | **p2p** }]

show bridge-domain vc-peer

Parameters

id

Specifies a unique numeric bridge-domain identifier. On SLX 9140, the range is from 1 through 4096. On SLX 9240, the range is from 1 through 3566.

logical-interface

Displays the operational information for logical interfaces configured under the bridge domain.

id

Specifies a logical interface instance ID.

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.

vc-peer

Causes the display of summary virtual connection (VC) peer information for the bridge domain.

Modes

Privileged EXEC mode.

Usage Guidelines

To display information about all bridge domains, specify the **bridge-domain** option without a bridge-domain identifier.

To display information about all logical interfaces configured under a specific bridge domain, specify the **logical-interface** option without a logical-interface identifier.

Examples

The following example shows the information displayed by the **show bridge-domain** command.

```
device# show bridge-domain
Bridge-domain 50
------------------------------
Bridge-domain Type: MP
Number of configured end-points: 2 , Number of Active end-points: 2
VE if-indx: 0, bpdu-drop-enable: TRUE
mac-limit: 0
VLAN: 5, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
Tagged Ports: po52.5
Un-tagged Ports:
VLAN: 4093, Tagged ports: 0(0 up), Un-tagged ports: 1 (1 up)
Tagged Ports:
Un-tagged Ports: po110.55
```

The following example displays the logical interface information for the bridge domain.

```
device# show bridge-domain 50 logical-interface
Bridge-domain 50
------------------------------
Bridge-domain Type: MP
AC LIF Count:  2 , VFI LIF Count: 0
           logical-interface eth0/11.5
           LIF ifindex: 0x2c4000c0, Service Instance: 0x5
           IVID:4658 (4658), Encap ID:1
           FLAG:6
                    bit  0 = 0 - LIF is TAGGED
                    bit  1 = 1 - Admin State is UP
                    bit  2 = 1 - LIF is L2
           Outer VLAN ID:5 (0x5), Inner VLAN ID:65535 (0xffff)
           Ingress Stats Index: Inv, Egress Stats Index: Inv
           logical-interface po110.55
           LIF ifindex: 0x2c800100, Service Instance: 0x37
           IVID:4658 (4658), Encap ID:1
           FLAG:86
                    bit  0 = 0 - LIF is TAGGED
                    bit  1 = 1 - Admin State is UP
                    bit  2 = 1 - LIF is L2
           Outer VLAN ID:5 (0x5), Inner VLAN ID:65535 (0xffff)
           Ingress Stats Index: Inv, Egress Stats Index: Inv
```

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: 2
Number of VPLS bridge-domains: 2
Macs Dynamically learned: 0, Macs statically configured: 0

 BDID(VC-ID)   TYPE             Intf (up)      Tunnels/PWs(up)    macs
               (T)-Transparent
 ==========    ===============  =========      ================   ====
   1(0)        MP               0(0)           2(0)               0
   2(0)        MP               0(0)           1(1)               0
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	The PWs and Tunnels columns for the **brief** option were merged.

show capabilities

Displays whether a variety of network services are enabled ("true") or not ("false").

Syntax

show capabilities

Modes

Privileged EXEC mode

Usage Guidelines

?

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show capture packet config

Displays the Online Packet Capture configuration.

Syntax

show capture packet config

Modes

Privileged EXEC mode

Examples

This example displays the Online Packet Capture configuration.

```
device# show capture packet config
%  All  protocol  RX capture is enabled on interface Eth 0/31
```

History

Release version	Command history
18s.1.01	This command was introduced.

show capture packet interface ethernet

Displays information about frames saved under Online Packet Capture.

Syntax

show capture packet interface ethernet *slot* **/** *port*

Parameters

slot

Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

This example displays information about the captured frames.

```
device# show capture packet interface ethernet 0/15
Packet Capture configured on the following interfaces
Eth 0/15
Frames Logged on interface Eth 0/15 :
-------------------------------------
Frame Received Time : Sat Jul 14 2018 19:18:46:216
Packet Type         :
Packet Direction    : RX
Interface info      : Eth 0/15
        ETHERNET HEADER
SrcMAC              : 0010.9400.0057
DstMAC              : 609c.9f87.4401
Tag Protocol ID     : 0x8100
VlanID              : 0x12c
```

History

Release version	Command history
18s.1.01	This command was introduced.

show cee maps

Displays the configuration information on the default CEE map with a list of all of the Layer 2 interfaces bound to the CEE map.

Syntax

show cee maps [**default**]

Parameters

default

The name of the only CEE map on the device.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays the CEE map.

```
device# show cee maps

CEE Map 'default'
   Precedence: 1
   Remap Lossless-Priority to Priority 0
   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:
```

History

Release version	Command history
17s.1.00	This command was introduced.

show cert-util ldapca

Displays the Lightweight Directory Access Protocol (LDAP) Certification Authority (CA) certificate.

Syntax

show cert-util ldapca

Modes

Privileged EXEC mode

Examples

To display the LDAP certificate on the device:

```
device# show cert-util syslogcacert
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

A typical output of this command:

```
device# show cert-util sshkey user testuser
user's public keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAtTCFzC1lfjwV9hjdtqv2ulSvmsmf7q7MS92Ctc3pDje/
YGYJPHVUi8bQX0XAsCAuzdsZL0BlVHdYPO1L4HStuIo8okfn4xLxrazqzwVeeL8p5Zcspf9zK8HmDzNpZ/
OuQ9MvfOuzbseYrovqgYLFGfPvY6vleFXZo61vVncFM7uFzasED9o9JUSBROhBki7vB0SG69yNn6ADnmpQW6QOu
+nYuZaWXO0QXk2OIB+hidjxSQVAfVLidSIGyfDD0go
+JAE3osxZxwQa5jcorASs4q2Gt4tSYERpvzOsjaAR5YivbmmBTIQWdUuR9Laz8s8VKF4Di9HQ4kE+xyBeAFNvQ==
bmeenaks@blc-10-6
```

History

Release version	Command history
17s.1.00	This command was introduced.

show cert-util syslogca

Displays the syslog Certification Authority (CA) certificate.

Syntax

show cert-util syslogca

Modes

Privileged EXEC mode

Examples

To display the syslog Certification Authority (CA) certificate on the device:

```
device# show cert-util ldapca

syslog CA
```

History

Release version	Command history
17s.1.00	This command was introduced.

show chassis

Displays the status for components in the chassis.

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.

Examples

The following example displays chassis information on a SLX 9140.

```
device# show chassis

Chassis Name:   BR-SLX9140
switchType: 3001

FAN  Unit: 1
Time Awake:             4 days

FAN  Unit: 2
Time Awake:             4 days

FAN  Unit: 3
Time Awake:             4 days

FAN  Unit: 4
Time Awake:             4 days

FAN  Unit: 5
Time Awake:             4 days

FAN  Unit: 6
Time Awake:             4 days

POWER SUPPLY  Unit: 1
Factory Part Num:
Factory Serial Num:
Time Awake:             0 days

POWER SUPPLY  Unit: 2
Factory Part Num:       23-1000076-01
Factory Serial Num:     EXA2T16M1AL
Time Awake:             4 days

CHASSIS/WWN  Unit: 1
Power Consume Factor:   0
Factory Part Num:       84-1002952-01
Factory Serial Num:     EXH3330M00M
Manufacture:            Day:  5  Month:  8  Year: 2016
Update:                 Day: 24  Month:  7  Year: 2017
Time Alive:             262 days
Time Awake:             4 days

Airflow direction : Port side INTAKE
```

History

Release version	Command history
17s.1.01	This command was introduced.

show cipherset

Displays the current cipherset status for LDAP and SSH.

Syntax

show cipherset

Modes

Privileged EXEC mode

Examples

To display cipherset status on the device:

```
device# show cipherset

LDAP Cipher List        : !DH:HIGH:-MD5
SSH Cipher List         : 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show cluster

Displays the MCT cluster information including client information.

Syntax

show cluster [*cluster-ID* [**client** *client-ID*]]

Parameters

cluster-ID

Specifies the cluster ID to display its configuration, peer, and client information.

client *client-ID*

Displays the specified client ID information.

Modes

Privileged EXEC mode

Command Output

The **show cluster** command displays the following information:

Output field	Description
Cluster State	Whether the cluster is deployed or undeployed
Client Isolation Mode	Client-isolation mode configuration: Strict or Loose
DF Hold Time	Designated hold time in seconds.
Configured Member Vlan Range	Configured VLANs as members to the MCT cluster.
Active Member Vlan Range	Active member VLANs.
Cluster Control Vlan	ID for the cluster control VLAN for MAC learning and resolving ARP for the BGP peer, and deriving the outer MAC address for the NSH tunnel.
No. of Peers	Number of configured peers.
No. of Clients	Number of configured clients.
Peer IP	Configured IP address for the MCT cluster peer.
Peer Interface	Configured peer interface slot and port.
Name	Configured client name.
ID	Configured client ID.
ESI	Configured Ethernet Segment ID (ESI) value .
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).

When you display a specified client ID, the following information is displayed.

Output field	Description
Client	Configured client name.

Output field	Description
Client-id	Configured client ID and whether it is deployed or undeployed.
Client state	Local and remote state of the client: Up or Down.
Interface state	State of the interface assigned to the client.
Interface	Configured interface assigned to the client.
Vlans	VLANs assigned to the client.
Bridge Domains	Number of bridge domains.
Number of DF Vlans	Number of designated forwarder VLANs.
Elected DF for vlans	Number of elected designated forwarder for the VLANs.
Number of DF Bridge Domains	Number of designated forwarder bridge domains.
Elected DF for Bridge Domains	Number of elected designated forwarder bridge domains.

Examples

The following example shows the information of the cluster on the SLX-OS device.

```
device# show cluster

Cluster MCT1 1
==============
Cluster State: Deploy
Client Isolation Mode: Strict
DF Hold Time: 3
Configured Member Vlan Range: 5, 100-1000
Active Member Vlan Range: 5,200,500-600, 800
Cluster Control Vlan: 4090
No. of Peers: 1
No. of Clients: 3

 Peer Info:
 ----------
 Peer IP: 10.10.10.20, State: Up

 Client Info:
 ------------
 Name     Id   ESI                           Interface    Local/Remote State
 access1  100  00.a1.b2.c3.d4.e5.f6.89.00     Eth 0/3          Up/UP
 access2  200  00.11.22.33.44.55.66.77.88     po-chan-2        Dep/UnDep
 access3  300  00.24.46.0e.cd.ab.66.16.00     Eth 0/8          Up/Down
```

History

Release version	Command history
17s.1.00	This command was introduced.

show cluster management

Displays the current state of an IP-based management cluster.

Syntax

show cluster management [**detail**]

Parameters

detail

Displays detailed information.

Modes

Privileged EXEC mode

Examples

The following example displays basic information regarding the IP-based management cluster.

```
device# show cluster management
CLUSTER ID                          : 2
Management Cluster UUID : 455451fd-205f-4482-87d4-4ed55944132c
Total Number of Nodes in Cluster    : 2

Node-Id         Switch MAC/WWN                IP Address       Status
_____________________________________________________________________
1               10:00:c4:f5:7c:50:06:2e       10.0.0.47        Co-ordinator
48              10:00:c4:f5:7c:50:06:2d       10.0.0.48        Connected
```

The following example displays detailed information.

```
device# show cluster management detail
Total Number of Nodes           :
Nodes Disconnected from Cluster :
Cluster Condition               : Good/Degraded
Cluster Status                  : All Nodes Present in the Cluster/Nodes Disconnected from Cluster
Node :1
    Serial Number :
    Condition     : Good
    Cluster Status    : Co-ordinator/ Connected to Cluster
    Node-Id    : 26*
    Co-ordinator  : YES
    Switch MAC    : 00:27:F8:DA:C4:86
    Switch Type   :
    Firmware Ver       :
    IP Address :  NA
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show cpu-interface

Displays information about the CPU Ethernet interface.

Syntax

show cpu-interface { **statistics interface backplane** }

Modes

Privileged EXEC mode

Examples

To display information about the CPU Ethernet interface:

```
device# show cpu-interface statistics interface backplane
Wave Management Interface Does Not Know The Client
```

History

Release version	Command history
17s.1.00	This command was introduced.

show crypto ca

Displays cryptographic trustpoint configuration information.

Syntax

show crypto ca { **trustpoint** | **certificates** }

Parameters

trustpoint

Causes the display of trustpoint configuration information.

certificates

Causes the display of certificate information. Both Certificate Authority (CA) certificate and identity certificate information is displayed.

Modes

Privileged EXEC mode

Usage Guidelines

Any keypair associated with a trustpoint is included in the trustpoint configuration information displayed by specifying the **trustpoint** parameter.

Command Output

The **show crypto ca** command displays the following information:

Output field		Description
Trustpoint		Trustpoint name
	key-pair	Name of the keypair associated with the trustpoint
CA certificate		
	SHA1 Fingerprint	Sequence of bytes used to identify the public key
	Subject	Name of the entity associated with the public key
	Issuer	Name of the entity that signed and issued the certificate
	Not Before	The beginning of the certificate validity period
	Not After	The end of the certificate validity period
	purposes	The purposes for which the certificate can be used

Examples

The following example displays trustpoint configuration information.

```
device# show crypto ca trustpoint

trustpoint: t1; key-pair: k1
```

The following example displays certificate configuration information.

```
device# show crypto ca certificates

Trustpoint: t1

CA certificate:
SHA1 Fingerprint=B7:5B:DB:9B:24:69:40:39:36:66:4D:59:2C:69:83:8E:93:CA:23:0C
Subject: C=US, ST=CA, L=SJ, O=BRC, OU=SFI, CN=10:00:00:27:F8:87:70:29
Issuer: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Not Before: Oct 6 23:44:27 2016 GMT
Not After : Oct 6 23:44:27 2017 GMT
purposes: sslserver

CA certificate:
SHA1 Fingerprint=76:5B:D4:2C:CB:54:FE:6B:C5:E0:E3:FD:11:B0:88:70:80:12:C6:63
Subject: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Issuer: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Not Before: Sep 19 20:56:49 2016 GMT
Not After : Oct 19 20:56:49 2016 GMT
purposes: sslserver
```

History

Release version	Command history
17s.1.00	This command was introduced.

show crypto key

Displays cryptographic key configuration information for HTTPS.

Syntax

show crypto key mypubkey

Parameters

mypubkey

Causes the display of public key configuration information.

Modes

Privileged EXEC mode

Command Output

The **show crypto key** command displays the following information:

Output field	Description
key type	Cryptographic key type. Supported key types include RSA, DSA and ECDSA.
key label	Cryptographic key label.
key size	Cryptographic key size.

Examples

The following example displays public key configuration information.

```
device# show crypto key mypubkey

key type: ecdsa
key label: k1
key size: 384
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command 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 0/1
 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 0/1
 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 0/1
 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 0/1
 Ethernet,     SrcMAC : 768e.f807.2005, DstMAC: 0010.9400.0001
 Internet proto, SrcIP : 11.1.1.1, DstIP: 11.1.1.2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

```
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
*****************************************
```

History

Release version	Command history
17s.1.00	This command was introduced.

show debug ip bgp all

Displays all BGP4 debugging options that are enabled.

Syntax

show debug ip bgp all

Modes

Privileged EXEC mode

Examples

```
device# show debug ip bgp all
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was modified to include the output example.

show debug ipv6 mld

Displays the IPv6 Multicast Listener Discovery (MLD) packets received and transmitted, as well as related events.

Syntax

show debug ipv6 mld

Modes

Privileged EXEC mode

Examples

The following example displays the output of the **show debug ipv6 mld** command.

```
device# show debug ipv6 mld

MLD debugging status:
---------------------------------------
errors          : on
group           : off
packets         : on
query           : on
report          : on
direction       : none
vlan            : none
l2_port         : none
```

History

Release version	Command history
17s.1.00	This command was introduced.

show debug ipv6 packet

Displays IPv6 packets captured through the packet capture utility on an interface or all interfaces, as well as the packet capture configuration on the switch.

Syntax

show debug ipv6 packet [**buffer** [**all** | **interface** [**ethernet** *slot/port*| **ve** *vlan_id*] [**rx** | **tx**]

Parameters

buffer
Specifies IPv6 packets.

all
Specifies all interfaces.

interface
Specifies an interface.

ethernet
Specifies an Ethernet port.

slot
Specifies a valid slot number. This must be **0** for devices that do not support line cards.

port
Specifies a valid port number.

ve*vlan_id*
Specifies a virtual Ethernet interface.

Command Default

None

Modes

Privileged EXEC mode

Examples

To display the current PCAP configuration on the switch:

```
device# show debug ipv6 packet
```

To display IPv6 packets captured on all interfaces:

```
device# show debug ipv6 packet buffer all
```

To display IPv6 packets captured on a specific Ethernet interface:

```
device# show debug ipv6 packet buffer interface ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

show debug lacp

Displays the status of Link Aggregation Control Protocol (LACP) debugging on the switch.

Syntax

show debug lacp

Modes

Privileged EXEC mode

History

Release version	Command history
17s.1.00	This command was introduced.

show debug lldp

Displays the status of Link Layer Discovery Protocol (LLDP) debugging on the switch.

Syntax

show debug lldp

Modes

Privileged EXEC mode

Examples

To display the status of LLDP debugging on the switch:

```
device# show debug lldp
 LLDP debugging status:
Interface Eth0/0    : Transmit Receive  Detail
```

History

Release version	Command history
17s.1.00	This command was introduced.

show debug spanning-tree

Displays the status of STP debugging flags on the switch.

Syntax

show debug spanning-tree

Modes

Privileged EXEC mode

History

Release version	Command history
17s.1.00	This command was introduced.

show debug vrrp

Displays the status of Virtual Router Redundancy Protocol (VRRP) debugging on the switch.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

1GLR
— 1G SFP LR

1GSR
— 1G SFP SR

10GER
— 10G SFP+ ER

10GLR
— 10G SFP+ LR

10GSR
— 10G SFP+ SR

10GUSR
— 10G SFP+ USR

10GZR
— 10G SFP+ ZR

25GSR
— 25G SFP+ SR

40GESR
— 40G QSFP+ eSR4 INT

40GLR
— 40G QSFP+ LR4

40GSR
— 40G QSFP+ SR4

40GSRINT
— 40G QSFP+ SR4 INT

100GCLR
— 100G QSFP28 CLR4

100GCWDM
— 100G QSFP28 CWDM4

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|
+------------+-------+--------+--------+-----------+------------+--------+
```

History

Release version	Command history
17s.1.00	This command was introduced.

show diag burninerrshow

Displays the error messages, stored in the device's nonvolatile memory, that were logged during failures in previous system-verification tests.

Syntax

show diag burninerrshow

Modes

Offline diagnostics mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

The log file is updated immediately by the system verification process when the **diag systemverification** command is executed.

Examples

The following example displays the output of this command.

```
diag<~>#  show diag burninerrshow
Running show diag burninerrshow ...
burninerr on round 1:
80:port loopback test on port 28 FAILED
88:port loopback test on port 32 FAILED
89:<<port loopback test on All port FAILED>>
burninerr on round 2:
80:port loopback test on port 28 FAILED
88:port loopback test on port 32 FAILED
89:<<port loopback test on All port FAILED>>
```

History

Release version	Command history
17s.1.00	This command was introduced.

show diag burninstatus

Displays the entire test log, from the last system-verification test, that is stored in the device's nonvolatile memory.

Syntax

show diag burninstatus

Modes

Offline diagnostics mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

The log file is updated immediately by the system verification process when the **diag systemverification** command is executed.

Examples

The follow example displays the output of this command.

```
diag<~># show diag burninstatus
Running show diag burninstatus ...
====================
date: Fri Feb 25 10:15:21 UTC 2000
systemverification on round 1
% Info: This test should be run to completion. Please do not abort while it is executing.
loop#1: PASS
memt -s 500 : PASSED
loop#1: PASS
memt -s 300 -a 1: PASSED
memtester.sh : PASSED
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portledtest...
[all LED on]
-- Done --
% Info: This test should be run to completion. Please do not abort while it is executing.
Running portloopbacktest...
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 1 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 2 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 3 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 4 PASSED

<---output truncated--->

Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 29 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 30 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 31 PASSED
Port type='MAC_MODE_4X10GB' link 'Up', Rx=100
port loopback test on port 32 PASSED
<<port loopback test on All port PASSED>>
```

History

Release version	Command history
17s.1.00	This command was introduced.

show diag revision

Displays the current version of the diagnostic software.

Syntax

show diag revision

Modes

Offline diagnostics mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

Examples

The following example displays output from this command.

```
diag<~>#  show diag revision
Diag version =1.2.3.90
```

History

Release version	Command history
17s.1.00	This command was introduced.

show diag setcycle

Displays parameters set for system verification.

Syntax

show diag setcycle

Modes

Offline diagnostics mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

The parameters can be modified by means of the **diag setcycle** command.

Examples

The following example displays the output of this command.

```
diag<~>#  show diag setcycle
Running show diag setcycle ...
CURRENT - KEYWORD : DEFAULT
0 - lb_mode : 0
2 - number_of_runs : 1
3 - pled_passes : 1
1 - tbr_passes : 1
100 - plb_nframes : 100
```

History

Release version	Command history
17s.1.00	This command was introduced.

show diag sysinfo

Displays system hardware information.

Syntax

show diag sysinfo

Modes

Offline diagnostics mode

Usage Guidelines

Refer to the "Diagnostic Commands" chapter in the *Extreme SLX-OS Management Configuration Guide*.

Examples

The following example displays system hardware information for a SLX 9240.

```
diag<~># show diag sysinfo
Running show diag sysinfo ...
Model =0x00000BB8 Cedar
SN =..........
CPU board CPLD revision =0x19
CPU board HW revision =0x03: [R01]
Main board FPGA revision =0x11
Main board CPLD revision =0x09 0x05 0x05
Main board PCB revision =0x00: [Version 1]
Main board HW revision =0x03:
```

The following example displays system hardware information for a SLX 9140.

```
diag<~># show diag sysinfo
Running show diag sysinfo ...
Model =0x00000BB9 Freedom
Model =0x00000BB9 Freedom
SN =..........
CPU board CPLD revision =0x19
CPU board HW revision =0x03: [R01]
Main board FPGA revision =0x11
Main board CPLD revision =0x09 0x05 0x05
Main board PCB revision =0x00: [Version 1]
Main board HW revision =0x03:
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 802.1X-related information for all ports on the device.

interface

Displays 802.1X-related status and configuration information for an interface.

ethernet *slot/port*

Specifies an Ethernet interface in slot number/port number format. When the device does not contain slots, the slot number must be 0 .

diagnostics

Displays 802.1X-related diagnostics information for the authenticator associated with a port.

session-info

Displays all 802.1X-related statistical information for an established session.

statistics

Displays the 802.1X-related statistics of a specified interface.

Modes

Privileged EXEC mode

Command Output

The **show dot1x** command displays the following information:

Output field		Description
802.1X Port-Based Authentication		Configuration status (Enabled or Disabled) for 802.1x port based authentication.
PAE Capability		Port Access Entity (PAE) role for the device. This is always "Authenticator Only".
Protocol Version		Version of the 802.1X protocol in use on the device.
Auth Server		Authentication server type; for example, RADIUS.
Readiness test timeout		802.1x readiness test timeout. The range is from 1 through 65535 seconds.
RADIUS Configuration		
	Position	Position of the configured RADIUS server.
	Server Address	IP address of the RADIUS server.

Output field		Description
	Port	Port on which 802.1X authentication is enabled.
	Secret	Secret key that is used to establish a connection between the RADIUS server and the device.
	Retry Interval	Authentication retry interval in seconds.
802.1X info for interface		
	Port Control	Port control type. The port control type may be: • Force Authorized—The controlled port is placed unconditionally in the authorized state, allowing all traffic. This is the default state. • Force Unauthorized—The controlled port is placed unconditionally in the unauthorized state. No authentication takes place for any connected 802.1X clients. • Auto—The authentication status for each 802.1X client depends on the authentication status returned by the RADIUS server.
	Port Auth Status	Port authentication status. The port authentication status may be: • Authorized—The port or MAC address is authenticated by the RADIUS server. • Unauthorized—The port or MAC address is not authenticated by the RADIUS server.
	Protocol Version	Version of the 802.1X protocol in use on the device.
	ReAuthentication	Periodic reauthentication status (Enabled or Disabled). When periodic reauthentication is enabled, the device automatically reauthenticates clients every 3,600 seconds by default.
	Auth Fail Max Attempts	Number of attempts to authenticate a client before taking the authentication failure action.
	ReAuth Max	Maximum number of reauthentication attempts.
	Tx Period	Time (in seconds) that the device waits before retransmitting the Extensible Authentication Protocol (EAP)-Request/Identity frame to a client after the client fails to send back an EAP-Response/Identity frame to a previous request. The default wait time is 30 seconds.
	Quiet Period	Time (in seconds) that the device waits before trying again to authenticate a client after a failed authentication attempt. The default wait time is 60 seconds.
	Supplicant Timeout	Time (in seconds) that the device waits before retransmitting an EAP-Request frame after the client fails to respond to a previous EAP-Request frame.
	Re-Auth Interval	Interval between reauthentication attempts (when reauthentication is enabled). The default interval is 3600 seconds.
802.1X Session info for interface		
	Mac Address	Supplicant MAC address.
	User Name	Supplicant user name.
	Session Time	Time (in seconds) elapsed since the session was authenticated by the RADIUS server.
	Terminate Cause	Reason for the session termination.
	Session Status	Session status (Authorized or Unauthorized).
	PAE State	State of the Authenticator PAE device. The state can be INITIALIZE, DISCONNECTED, CONNECTING, AUTHENTICATING, AUTHENTICATED, ABORTING, HELD, FORCE_AUTH, or FORCE_UNAUTH.
	BE State	State of the backend authentication state-machine.
	Current Id	Session ID that is currently being sent to the RADIUS server to establish connection.
	Id From Server	ID that is returned by the RADIUS server.
802.1X statistics for interface		
	EAPOL Frames Rx	Total number of Extensible Authentication Protocol over LAN (EAPOL) frames received on the port.
	EAPOL Frames Tx	Total number of EAPOL frames transmitted on the port.

Output field		Description
	EAPOL Start Frames Rx	Number of EAPOL Start frames received on the port.
	EAPOL Logoff Frames Rx	Number of EAPOL Logoff frames received on the port.
	EAP Rsp/Id Frames Rx	Number of EAP-Response/Identity frames received on the port.
	EAP Response Frames Rx	Number of EAP-Response frames transmitted on the port that were not EAP-Response/Identity frames.
	EAP Req/Id Frames Tx	Number of EAP-Request/Identity frames received on the port.
	EAP Request Frames Tx	Number of EAP-Request frames transmitted on the port that were not EAP-Request/Identity frames.
	Invalid EAPOL Frames Rx	Number of invalid EAPOL frames received on the port.
	EAPOL Length Error Frames Rx	Number of EAPOL frames received on the port that have an invalid packet-body length.
	EAPOL Last Frame Version Rx	Version number of the last EAPOL frame received on the port.
	Invalid EAP Frames Rx	Number of invalid EAP frames received on the port.
	EAP Length Error Frames Rx	Number of EAP frames received on the port that have an invalid packet-body length.
	EAPOL Last Frame Src	Source MAC address in the last EAPOL frame received on the port.
802.1X Diagnostics for interface		
	authEnterConnecting	Number of EAP Frames received on connecting state.
	authEaplogoffWhileConnecting	Number of EAP frames logged off while connecting.
	authEnterAuthenticating	Number of EAP Frames received on authenticating state.
	authSuccessWhileAuthenticating	Number of authenticated EAPOL frames.
	authTimeoutWhileAuthenticating	Number of timed-out EAPOL frames during authentication process.
	authFailWhileAuthenticating	Number of failed EAPOL frames during authentication process.
	authEapstartWhileAuthenticating	Number of transitions from AUTHENTICATING to ABORTING states, as a result of an EAPOL-Start message being received from the Supplicant.
	authEaplogoffWhileAuthenticating	Number of transitions from AUTHENTICATING to ABORTING states, as a result of an EAPOL-Logoff message being received from the Supplicant.
	authReauthsWhileAuthenticated	Number of t transitions from AUTHENTICATED to CONNECTING states, as a result of a reauthentication request.
	authEapstartWhileAuthenticated	Number of transitions from AUTHENTICATED to CONNECTING states, as a result of an EAPOL-Start message being received from the Supplicant.
	authEaplogoffWhileAuthenticated	Number of transitions from AUTHENTICATED to DISCONNECTED states, as a result of an EAPOL-Logoff message being received from the Supplicant.
	BackendResponses	Number of times that the state machine sends an initial Access-Request packet to the Authentication server; that is, executes sendRespToServer on entry to the RESPONSE state which indicates that the Authenticator attempted communication with the Authentication server.
	BackendAccessChallenges	Number of times that the state machine receives an initial Access-Challenge packet from the Authentication server; that is, aReq becomes TRUE, causing exit from the RESPONSE state which indicates that the Authentication server is in communication with the Authenticator.
	BackendOtherrequestToSupplicant	Number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure or Success message) to the Supplicant; that is, executes txReq on entry to the REQUEST state which indicates that the Authenticator chose an EAP-method.
	BackendAuthSuccess	Number of times that the state machine receives an EAP-Success message from the Authentication Server; that is, aSuccess becomes TRUE causing a transition from RESPONSE to SUCCESS which indicates that the Supplicant is successfully authenticated to the Authentication Server.

Output field		Description
	BackendAuthFails	Number of times that the state machine receives an EAP-Failure message from the Authentication Server; that is, aFail becomes TRUE causing a transition from RESPONSE to FAIL which indicates that the Supplicant is not authenticated to the Authentication Server.

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 0/31
---------------------------------
Port Control:             Force Authorized
Port Auth Status:         Unauthorized
Protocol Version:         2
ReAuthentication:         Disabled
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
```

The following example shows state of a specified interface.

```
device# show dot1x interface ethernet 0/31

802.1X info for interface Eth 0/31
---------------------------------
Port Control:             Force Authorized
Port Auth Status:         Unauthorized
Protocol Version:         2
ReAuthentication:         Disabled
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
```

The following example shows information for all clients on the port.

```
device# show dot1x session-info interface ethernet 0/2

802.1X Session info for interface Eth 0/2
----------------------------------------
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
Current Id:               18
Id From Server:           17
```

The following example shows the statistics of a specified interface.

```
device# show dot1x statistics interface ethernet 0/2
802.1X statistics for interface Eth 0/2
---------------------------------------
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
```

The following example shows all diagnostics information for the authenticator associated with a port.

```
device# show dot1x diagnostics interface ethernet 0/2
802.1X Diagnostics for interface Eth 0/2
----------------------------------------
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show environment fan

Displays fan status information.

Syntax

show environment fan

Modes

Privileged EXEC mode

Command 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 5677 RPM
Fan 2 is Ok, speed is 5677 RPM
Fan 3 is Ok, speed is 5677 RPM
Fan 4 is Ok, speed is 5677 RPM
Fan 5 is Ok, speed is 5857 RPM
Fan 6 is Ok, speed is 5677 RPM
Airflow direction : Port side INTAKE
```

History

Release version	Command history
17s.1.00	This command was introduced.

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) or chassis ID (CID) cards. The type of FRU supported depends on the hardware platform.

Command Output

The **show environment history** command displays the following information:

Output field	Description
Object type	On standalone platforms: FAN, POWER SUPPLY, WWN (WWN card), or UNKNOWN.
Object number	Displays the slot number for blades. Displays the unit number for all other object types.
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 (xxxxxxxxxxx) or Not available.

Examples

The following example displays the FRU history on a device.

```
device# show environment history
FAN  Unit 1  Inserted at Wed Feb 16 20:51:32 2000
Factory Part Number:   Not Available
Factory Serial Number: Not Available

FAN  Unit 2  Inserted at Wed Feb 16 20:51:32 2000
Factory Part Number:   Not Available
Factory Serial Number: Not Available

FAN  Unit 3  Inserted at Wed Feb 16 20:51:32 2000
Factory Part Number:   Not Available
Factory Serial Number: Not Available

FAN  Unit 4  Inserted at Wed Feb 16 20:51:32 2000
Factory Part Number:   Not Available
Factory Serial Number: Not Available

FAN  Unit 5  Inserted at Wed Feb 16 20:51:32 2000
Factory Part Number:   Not Available
Factory Serial Number: Not Available

FAN  Unit 6  Inserted at Wed Feb 16 20:51:33 2000
Factory Part Number:   Not Available
Factory Serial Number: Not Available

POWER SUPPLY  Unit 1  Inserted at Wed Feb 16 20:51:33 2000
Factory Part Number:   23-1000076-01
Factory Serial Number: D1616RA0451

POWER SUPPLY  Unit 2  Inserted at Wed Feb 16 20:51:34 2000
Factory Part Number:   Not Available
Factory Serial Number: Not Available

Records:  8
```

History

Release version	Command history
17s.1.00	This command was introduced.

show environment power

Displays the type and current status of the switch power supply.

Syntax

show environment power

Modes

Privileged EXEC mode

Command Output

The **show environment power** command displays the following information:

Output field	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).
Airflow	Direction of fan air flow.

Examples

The following example displays the power supply status.

```
device# show environment power

Power Supply #1 is absent
Power Supply #2 is OK
2T,23-1000076-01,EXA2T28L015,AirFlow: Port Side Intake
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** command.

Examples

The following example displays sensor readings on the device:

```
device# show environment sensor
sensor  1: (Temperature) is Ok, value is 34 C
sensor  2: (Temperature) is Ok, value is 34 C
sensor  3: (Temperature) is Ok, value is 33 C
sensor  4: (Temperature) is Ok, value is 32 C
sensor  5: (Fan         ) is Ok,speed is 5677 RPM
sensor  6: (Fan         ) is Ok,speed is 5857 RPM
sensor  7: (Fan         ) is Ok,speed is 5857 RPM
sensor  8: (Fan         ) is Ok,speed is 5677 RPM
sensor  9: (Fan         ) is Ok,speed is 5857 RPM
sensor 10: (Fan         ) is Ok,speed is 5677 RPM
sensor 11: (Power Supply) is Ok
sensor 12: (Power Supply) is Faulty
```

History

Release version	Command history
17s.1.00	This command was introduced.

show environment temp

Displays environment temperature.

Syntax

show environment temp

Modes

Privileged EXEC mode

Command Output

The **show environment temp** command displays the following information:

Output field	Description
Sensor ID	Displays the sensor ID.
Sensor state	Displays OK, Above maximum, or Absent.
Temperature	Display the temperature in Centigrade and Fahrenheit.

Examples

The following example displays temperature readings on a the device.

```
device# show environment temp

Sensor  State           Centigrade     Fahrenheit
  ID
================================================
  1     Ok                  36             96
  2     Ok                  40            104
  3     Ok                  32             89
```

History

Release version	Command history
17s.1.00	This command was introduced.

show event-handler activations

Displays operational data of activated event-handlers.

Syntax

show event-handler activations

Modes

Privileged EXEC mode

Command 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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
!

protocol lldp
!!
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging auditlog class SECURITY
!
end
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 (0), 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  17s.1.01
2      Wed Feb 22 17:10:45 2017   SLX          0     3187   17s.1.00
```

History

Release version	Command history
17s.1.00	This command was introduced.

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]: Thu Mar  2 05:51:50 2017
Slot SW/0: Firmware install begins.
[2]: Thu Mar  2 05:56:18 2017
Slot SW/0: Firmware install ends.
[3]: Thu Mar  2 05:56:18 2017
Slot SW/0: Firmware starts to swap.
[4]: Thu Mar  2 05:56:22 2017
Slot SW/0: Firmware is swapped.
[5]: Thu Mar  2 05:56:22 2017
Slot SW/0: The blade begins to reboot.
[6]: Thu Mar  2 06:00:14 2017
Slot SW/0: The blade is rebooted.
[7]: Thu Mar  2 06:00:14 2017
Slot SW/0: Firmware commit begins.
[8]: Thu Mar  2 06:02:51 2017
Slot SW/0: Firmware commit ends.
[9]: Thu Mar  2 06:02:51 2017
Slot SW/0: Firmware is downloaded successfully.
```

The following example displays a high-level summary of the firmware download status.

```
device# show firmwaredownloadstatus summary
No Firmware Download session in progress.
```

History

Release version	Command history
17s.1.00	This command was introduced.

show hardware profile

Displays details of the current active hardware profile. You can also display details for a specified TCAM, route-table, or IPv6-lookup profile.

Syntax

show hardware profile [**current**]

show hardware profile route-table { **default** | **ipv4-max-arp** | **ipv6-max-nd** | **multicast** | **multicast-snoop** | **user-defined** }

show hardware profile ipv6-lookup { **default** | **network-id** }

show hardware profile overlay-visibility { **default** | **endpoint** | **endpoint-vni** | **tunnel-vni** | **vni** }

(SLX 9140) **show hardware profile tcam** { **default** | **l2-acl-l3-iacl** | **l2-iacl-l3-acl** | **l2-l3-iacl-l2-iqos** | **l2-l3-iqos-l2-eacl** | **l2-l3-iqos-l2-iacl** | **l2-l3-iqos-l3-eacl** | **l2-l3-iqos-l3-iacl** | **user-defined** }

(SLX 9240) **show hardware profile tcam** { **default** | **l2-l3-iacl** | **l2-l3-iqos** | **l3-acl** | **l3-iacl-l2-eacl** | **l3-iacl-l2-iqos** | **l3-iqos-l2-iacl** | **user-defined** }

Parameters

current
Displays details of the current active profile.

ipv6-lookup
(NPB system-mode) Displays details of the IPv6 address lookup-mode.

default
Displays details of the default IPv6 address lookup-mode.

network-id
Displays details of the network-id IPv6 address lookup-mode.

overlay-visibility
(Default system-mode) Displays overlay-visibility profile information.

default
Matches on outer source IP and destination IP.

endpoint
Matches on outer source IP or destination IP.

endpoint-vni
Matches on outer source IP and VNI or destination IP and VNI.

tunnel-vni
Matches on outer source IP, destination IP, and VNI.

vni
Matches on VNI only.

route-table
(Default system-mode) Specifies hardware resources for route profiles.

default
Specifies IPv4/IPv6 resources for dual-stack operations.

ipv4-max-arp
Specifies resources for the maximum number of IPv4 ARP entries.

ipv6-max-nd
Specifies resources for the maximum number of IPv6 Neighbor Discovery entries.

multicast
Specifies resources for IP unicast dual-stack and IPv4 mulitcast.

multicast-snoop
Specifies resources for IP unicast dual-stack and multicast snooping.

user-defined
Specifies resources for a user-defined profile.

tcam (SLX 9140)
Specifies hardware resources for TCAM profiles.

default
Specifies resources with basic support for all applications.

l2-acl-l3-iacl
Specifies resources for ingress and egress Layer 2 ACLs; and ingress IPv4 and IPv6 ACLs.

l2-iacl-l3-acl
Specifies resources for ingress Layer 2 ACLs; and ingress and egress IPv4 and IPv6 ACLs.

l2-l3-iacl-l2-iqos
Specifies resources for ingress Layer 2, IPv4, and IPv6 ACLs; and ingress Layer 2 QoS.

l2-l3-iqos-l2-eacl
Specifies resources for ingress Layer 2, IPv4, and IPv6 QoS; and egress Layer 2 ACLs.

l2-l3-iqos-l2-iacl
Specifies resources for ingress Layer 2, IPv4, and IPv6 QoS; and ingress Layer 2 ACLs.

l2-l3-iqos-l3-eacl
Specifies resources for ingress Layer 2, IPv4, and IPv6 QoS; and egress IPv4 and IPv6 ACLs.

l2-l3-iqos-l3-iacl
Specifies resources for ingress Layer 2, IPv4, and IPv6 QoS; and ingress IPv4 and IPv6 ACLs.

user-defined
Specifies resources for a user-defined TCAM profile.

tcam (SLX 9240)
Specifies hardware resources for TCAM profiles.

default
Specifies resources with basic support for all applications.

l2-l3-iacl
Specifies resources for ingress Layer 2, IPv4, and IPv6 ACLs.

l2-l3-iqos
Specifies resources for ingress Layer 2, IPv4, and IPv6 QoS.

l3-acl
Specifies resources for ingress and egress IPv4 and IPv6 ACLs.

l3-iacl-l2-eacl
Specifies resources for egress Layer 2 ACLs; and ingress IPv4 and IPv6 ACLs.

l3-iacl-l2-iqos
Specifies resources for ingress Layer 2 QoS; and ingress IPv4 and IPv6 ACLs.

l3-iqos-l2-iacl
Specifies resources for ingress Layer 2 ACLs; and ingress IPv4 and IPv6 QoS.

user-defined
(Default system-mode only) Specifies resources for a user-defined TCAM profile.

Modes

Privileged EXEC mode

Usage Guidelines

Local hardware profile information can be obtained by means of the **current** keyword.

Route-table profiles are supported only in default system-mode, not in network packet broker (NPB) mode.

In NPB mode, the only TCAM profile supported is the default TCAM profile.

IPv6 address profiles are supported only NPB mode. For implementation details, refer to the **profile ipv6-lookup** topic.

Examples

(Default system-mode) The following example displays details of the current active profile.

```
device# show hardware profile current
 switch type: BR-SLX9240
 system mode: Default
                     current TCAM profile:    L2-L3-IACL
_____________________________________________________________
 MAC ACL Based QoS Policy Entries (Ingress):    0
         MAC Security ACL Entries (Ingress):    512
        MAC Policy Based forwarding entries:    0
IPV4 ACL Based QoS Policy Entries (Ingress):    0
IPV4 Policy Based Routing Entries (Ingress):    0
        IPV4 Security ACL Entries (Ingress):    0
IPV6 Policy Based Routing Entries (Ingress):    0
IPV6 ACL Based QoS Policy Entries (Ingress):    0
        IPV6 Security ACL Entries (Ingress):    0
          IP Security ACL Entries (Ingress):    512
  IP ACL Based QoS Policy Entries (Ingress):    0
          MAC Security ACL Entries (Egress):    0
  MAC ACL Based QoS Policy Entries (Egress):    0
         IPV4 Security ACL Entries (Egress):    0
 IPV4 ACL Based QoS Policy Entries (Egress):    0
         IPV6 Security ACL Entries (Egress):    0
 IPV6 ACL Based QoS Policy Entries (Egress):    0
           IP Security ACL Entries (Egress):    0
   IP ACL Based QoS Policy Entries (Egress):    0
_____________________________________________________________
                      current ROUTE profile:    DEFAULT
                              Maximum paths:    8
_____________________________________________________________
                        IPV4 neighbor cache:    10240
                        IPV6 neighbor cache:    4608
         IPV4 multicast multi-source groups:    512
         IPV4 multicast single-source group:    1024
                            Max IPV4 routes:    49152
                            Max IPV6 routes:    8192
                              Max next hops:    2048
                              L2 Forwarding:    29696
                      IPV4 multicast snoop:     1024
                      IPV6 multicast snoop:     512
                                    Vlans:      2048
                                  My MAC:       2048
```

The following example displays specific route-table information about resource allocation, facilitating management.

```
device# show hardware profile route-table ipv4-max-arp
 switch type: BR-SLX9240
 system mode: Default
                               ROUTE profile:    IPV4_MAX_ARP
_____________________________________________________________
                        IPV4 neighbor cache:    16384
                        IPV6 neighbor cache:    0
         IPV4 multicast multi-source groups:    0
         IPV4 multicast single-source group:    0
                            Max IPV4 routes:    49152
                            Max IPV6 routes:    8192
                              Max next hops:    2048
                              L2 Forwarding:    29696
                      IPV4 multicast snoop:     0
                      IPV6 multicast snoop:     0
                                    Vlans:      4096
                                  My MAC:       2048
_____________________________________________________________
```

The following example displays typical NPB information.

```
device# show hardware profile current

 switch type: BR-SLX9140
 system mode: NPB

                      current TCAM profile:    DEFAULT
_____________________________________________________________
        MAC Policy Based forwarding entries:    2048
    IP Policy Based Forwarding Entries (Ingress):    2048
    Flex Policy Based Forwarding Entries (Ingress):    1024
_____________________________________________________________
        current IPv6-Address Profile:    NETWORK-ID
_____________________________________________________________
    Valid IPv6 Source Address Bits: 0-63
    Valid IPv6 Destination Address Bits: 0-63
_____________________________________________________________
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified to display default or network packet broker (NPB) system-mode.
18s.1.00	Under NPB system-mode, this command was modified to display default (host ID) or network-ID IPv6-address mode.

show hardware profile overlay-visibility

Displays hardware profile information related to overlay visibility.

Syntax

show hardware profile overlay-visibility { **default** | **endpoint** | **endpoint-vni**| **tunnel-vni**| **vni**}

Parameters

default
Displays a match on outer source IP and destination IP addresses.

endpoint
Displays a match on outer source IP or destination IP addresses.

endpoint-vni
Displays a match on outer source IP address and virtual network identifier (VNI), or destination IP address and VNI.

tunnel-vni
Displays a match on outer source IP address, destination IP address, and VNI.

vni
Displays a match on VNI only.

Modes

Privileged EXEC mode

Usage Guidelines

The options above are configured by the **profile overlay-visibility** command.

Examples

The following example displays a match on VNI only.

```
device# show hardware profile overlay-visibility vni
 switch type: BR-SLX9140
 system mode: Default
                Overlay Visibility Profile:    VNI
_____________________________________________________________
                                     VNI:    32768
_____________________________________________________________
```

History

Release version	Command history
17s.1.01	This command was introduced.

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 four last commands entered.

```
device# show history 4
12:45:06 -- show hardware port-group
12:45:23 -- show interface switchport
12:45:37 -- show interface stats brief
12:45:45 -- show arp vrf test
```

History

Release version	Command history
17s.1.00	This command was introduced.

show http server status

Displays HTTP and HTTPS server status information.

Syntax

show http server status

Modes

Privileged EXEC mode

Command 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show inner-gtp-https

Displays a list of all interfaces on which the dropping of GPRS Tunneling Protocol (GTP) frames that encapsulate HTTPs packets is enabled.

Syntax

show inner-gtp-https

Modes

Privileged EXEC mode

Examples

The following example indicates that this feature is enabled on an Ethernet interface.

```
device# show inner-gtp-https
interface Ethernet 0/23
    deny inner-gtp-https
```

History

Release version	Command history
17s.1.02	This command was introduced.

show interface

Displays the detailed interface configuration and capabilities of all interfaces or for a specified interface.

Syntax

show interface [**description**]

show interface [**ethernet** *slot* **/** *port* | **port-channel** *number*] [**switchport**]

show interface loopback *number*

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. Must be 0 if the switch does not contain slots.

port
Specifies a valid port number.

port-channel *number*
Specifies a port-channel number. Depending on the platform, valid values range from 1 through 1024.

switchport
Specifies Layer 2 interfaces.

loopback *number*
Specifies a loopback interface.

trunk
Displays VLANs on the trunk.

Modes

Privileged EXEC mode

Command 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)".
Hardware	Displays the MAC address of the Ethernet interface.
Pluggable media	Displays "present" or "not present".

Output field	Description
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.
LineSpeed Actual	Displays the actual line speed in Mb or "Nil".
Transparent phy loopback	(Under NPB) If the interface is in transparent loopback mode, displays "configured".
LineSpeed Configured	Displays "Auto" or a value in Mb.
Duplex	Displays "Half" or "Full".
Priority Tab	Displays "enable" or "disable".
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".
FEC Mode	Displays the forward error correction (FEC) mode: "RS-FEC", "FC-FEC", "Auto-Negotiation" or "disabled".
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.
Time since last interface status change	In days, hours, and minutes, displays time elapsed since the last interface status change.

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.

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 "loopback".
Pluggable media	Displays "present" or "not present".
Interface index	Displays the interface index.
IP 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.
FEC Mode	Displays the forward error correction (FEC) mode: "RS-FEC", "FC-FEC", "Auto-Negotiation" or "disabled".

The **show interface 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 Vlan	Displays the ID number of the active VLAN.

Examples

The following example displays detailed information for the Ethernet interface 0/1.

```
device# show interface ethernet 0/1
Ethernet 0/1 is admin down, line protocol is down (admin down)
Hardware is Ethernet, address is 609c.9f87.2205
    Current address is 609c.9f87.2205
Pluggable media present
Interface index (ifindex) is 201335040
MTU 1548 bytes
100G Interface
LineSpeed Actual     : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Last clearing of show interface counters: 1d18h07m
Queueing strategy: fifo
FEC Mode - RS-FEC
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:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, 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
Time since last interface status change: 1d18h07m
```

The following example displays a list of VLANs allowed on the trunk, per interface.

```
device# show interface trunk
-----------------------------------------------
Port        Vlans Allowed on Trunk
-----------------------------------------------
Eth 0/1    Nil
Eth 0/2    101

(Output truncated)

Eth 0/31           Nil
Eth 0/32           Nil
Po 26              1, 201-211, 225, 230, 235-249,
```

The following example displays details of Layer 2 interfaces.

```
device# show interface switchport
Interface name:          Ethernet 0/8
Switchport mode:         access
Ingress filter:          enable
Acceptable frame types: vlan-untagged only
Default Vlan:            101
Active Vlans:            101

Interface name:          Ethernet 0/21
Switchport mode:         trunk
Ingress filter:          enable
Acceptable frame types: vlan-tagged only
Native Vlan:             1
Active Vlans:            1,201-210,245-250,4090

Interface name:          Ethernet 0/25
Switchport mode:         trunk
Ingress filter:          enable
Acceptable frame types: vlan-tagged only
Native Vlan:             1
Active Vlans:            1,201-210,245-250

Interface name:          Ethernet 0/27
Switchport mode:         access
Ingress filter:          enable
Acceptable frame types: vlan-tagged only
Native Vlan:             240
Active Vlans:            240

Interface name:          Ethernet 0/31
Switchport mode:         trunk-no-default-native
Ingress filter:          enable
Acceptable frame types: vlan-tagged only
Native Vlan:             -
Active Vlans:
```

The following example details of a specified loopback interface.

```
device# show interface loopback 11
Loopback 11 is up, line protocol is up
Hardware is Loopback
Pluggable media not present
Interface index (ifindex) is 1476395019
IP MTU 1500 bytes
LineSpeed Actual
LineSpeed Configured: Auto
Last clearing of show interface counters: 00:00:38
Queueing strategy: fifo
Primary Internet Address is 10.10.10.10/32
FEC Mode - Disabled
```

History

Release version	Command history
17s.1.00	This command was introduced.

show interface port-channel

Displays the status of a port-channel.

Syntax

show interface port channel { *number* }

Parameters

number

Port-channel number. Range is from 1 through 1024.

Modes

Privileged EXEC mode

Examples

The following example displays the status of a port-channel.

```
device# show interface port channel 10
Port-channel 10 is admin down, line protocol is down (admin down)
Hardware is AGGREGATE, address is 609c.9fb1.4a4f
    Current address is 609c.9fb1.4a4f
Interface index (ifindex) is 671088650
Minimum number of links to bring Port-channel up is 1
MTU 1548 bytes
LineSpeed Actual     : Nil
Allowed Member Speed : 100000 Mbit
Priority Tag disable
Last clearing of show interface counters: 11:38:47
Queueing strategy: fifo
FEC Mode - Disabled
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:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, 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
Time since last interface status change: 11:38:46
```

History

Release version	Command history
17s.1.01	This command was introduced.

show interface stats

Displays a brief or detailed list of interface statistics. You can display such lists either for all interfaces or for a specified interface.

Syntax

show interface stats brief

show interface stats detail [**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. Must be 0 if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel number. Depending on the platform, valid values range from 1 through 1024.

Modes

Privileged EXEC mode

Examples

The following example displays detailed statistics for a specified Ethernet interface.

```
device# show interface stats detail interface ethernet 0/25

 Interface Ethernet 0/25 statistics (ifindex 413007892)
                                RX                              TX
             Packets        15069980                        38855
               Bytes     18850526482                      4892750
             Unicasts        15027331                            1
          Multicasts           42423                        38853
          Broadcasts             210                            1
              Errors               0                            0
            Discards               0                            0
            Overruns               0       Underruns            0
               Runts               0
              Jabbers              0
                 CRC               0
        64-byte pkts               0
   Over 64-byte pkts            7092
  Over 127-byte pkts         1876809
  Over 255-byte pkts         1229162
  Over 511-byte pkts             168
 Over 1023-byte pkts        11956733
 Over 1518-byte pkts               0
           Mbits/Sec        0.174379                     0.001014
          Packet/Sec              94                            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 25

 Interface Port-channel 25 statistics (ifindex 671088665)
                                RX                              TX
             Packets              21                           53
               Bytes            2784                         7024
             Unicasts               0                            0
          Multicasts              21                           53
          Broadcasts               0                            0
              Errors               0                            0
            Discards               0                            0
            Overruns               0       Underruns            0
               Runts               0
              Jabbers              0
                 CRC               0
        64-byte pkts               0
   Over 64-byte pkts               2
  Over 127-byte pkts              19
  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%
```

The following example displays brief statistics for the device.

```
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show interface status

Displays the status of all device interfaces.

Syntax

show interface status

Modes

Privileged EXEC mode

Command 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", "Trunk", or no value.
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 0/1      adminDown       --         --       --
Eth 0/2      adminDown       --         --       --
Eth 0/3      adminDown       --         --       --
...
Eth 0/15     connected (up)  Access     10G      10G-SFP-SR                    -
...
(output
               truncated)
```

History

Release version	Command history
17s.1.00	This command was introduced.

show inventory

Displays the hardware inventory of the device.

Syntax

show inventory [**chassis** | **fan** | **module** | **powerSupply**]

Parameters

chassis
Displays information about the chassis.

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
show inventory chassis
NAME: Chassis  DESCR:System Chassis
SID:BR-SLX9240     SwitchType:3000
PN:84-1002941-01  SN:EXG3319N00J
SLX# show inventory chassis
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 4 DESCR:Chassis Fan module
PN:N/A            SN:N/A
NAME:FAN 5 DESCR:Chassis Fan module
PN:N/A            SN:N/A
NAME:FAN 6 DESCR:Chassis Fan module
PN:N/A            SN:N/A
NAME:POWER SUPPLY 2 DESCR:Chassis PS module
PN:23-1000076-01  SN:EXA2T28L015
NAME: Chassis  DESCR:System Chassis
SID:BR-SLX9240     SwitchType:3000
PN:84-1002951-01  SN:EXG3319M00J
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip anycast-gateway

Displays details for IPv4 anycast gateway for all or specified virtual Ethernet (VE) interfaces or VRF instances.

Syntax

show ip anycast-gateway [**interface** *VE* | **vrf** *VRF-name*]

Parameters

interface *VE*
Specifies a VE interface.

vrf *VRF-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

To display details for IPv4 anycast gateway for all VE interfaces:

```
device# show ip anycast gateway
Gateway mac: 000a.000b.000c
interface     ip address        state
ve10          2.2.2.2/24        Active
ve10          2.2.3.2/24        Active
ve20          3.3.3.3/24        Active
```

To display details for IPv4 anycast gateway for a specified VE interface:

```
device# show ip anycast-gateway interface ve 10
Gateway mac: 000a.000b.000c
interface     ip address        state
ve10          2.2.2.2/24        Active
ve10          2.2.3.2/24        Active
```

History

Release version	Command history
17s.1.01	This command was introduced.

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

Command 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.
ACL Logging	Does not display a value.

Examples

The following example displays DAI information for all VLANs.

```
device# show ip arp inspection
  Vlan  Configuraton     Operation     ACL Match   ACL Logging
-------------------------------------------------------------------------------
     1       Enabled        Active
    10      Disabled      Inactive
   100       Enabled        Active          acl1
    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   ACL Logging
-------------------------------------------------------------------------------
     1       Enabled        Active
   100       Enabled        Active          acl1
  1000       Enabled        Active
   200      Disabled      Inactive
  2000       Enabled        Active          acl1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Must be `0` if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

Modes

Privileged EXEC mode

Usage Guidelines

On VLANs enabled for Dynamic ARP Inspection (DAI), interfaces not listed in the command output are untrusted.

Command 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 60        Trusted
Eth 0/1       Trusted
Eth 0/2       Trusted
--------------------------------------

All other interfaces are untrusted.
```

The following example displays the trust state of Ethernet interface 0/1.

```
device# show ip arp inspection interfaces ethernet 0/1
Interface     Trust State
--------------------------------------
Eth 0/1       Trusted
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip arp inspection statistics

Displays dynamic ARP inspection (DAI) statistics for one or more DAI-enabled VLANs.

Syntax

show ip arp inspection statistics [**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 1 through 4090.

Modes

Privileged EXEC mode

Command Output

The **show ip arp inspection statistics** command displays the following information:

Output field	Description
Vlan	Displays the VLAN name.
Forwarded	Displays packets forwarded, included packets permitted by ARP ACLs.
Dropped	Displays packets dropped as a result of DAI policy.
ACL Permit	Displays packets forwarded based on **permit** statements in ARP ACLs.

Examples

The following example displays statistics for VLAN 400.

```
device# show ip arp inspection statistics vlan 400
   Vlan     Forwarded       Dropped    ACL Permit
-------------------------------------------------------
    400             0             0             0
```

The following example displays statistics for all DAI-enabled VLANs.

```
device# show ip arp inspection statistics

 Vlan      Forwarded        Dropped     ACL Permit
-------------------- ------------------------------
    1              0             0        0
    2              0             0        0
    3          68322        220356    68322
    4              0             0        0
  100              0             0        0
  101              0             0        0
 1006              0             0        0
 1007              0             0        0
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip arp suppression-cache

Displays IPv4 ARP-suppression information.

Syntax

show ip arp suppression-cache [**summary**]

show ip arp suppression-cache bridge-domain *bridge-domain-id*

show ip arp 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

Command Output

The **show ip arp 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 IP 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.
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 ip arp suppression-cache
Flags: L  - Locally Learnt Adjacency
       R  - Remote Learnt Adjacency
       RS - Remote Static Adjacency
Vlan/Bd  IP         Mac            Interface                  Age       Flags
-------------------------------------------------------------------------------
4003 (V) 40.3.1.100 00ec.4003.3401 Eth 0/41                   03:09:44  L
4003 (V) 40.3.1.101 00ec.4003.3402 Eth 0/41                   03:09:44  L
4007 (V) 40.7.1.100 00ec.4007.4401 Tu 61441 (114.114.114.114) Never     R
4007 (V) 40.7.1.101 00ec.4007.4402 Tu 61441 (114.114.114.114) Never     R
467  (V) 4.67.1.6   609c.9f70.1e01 Nsh Eth 0/1                Never     RS
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip as-path-list

Displays the status of AS-path access control lists (ACLs).

Syntax

show ip as-path-list *list_name*

Parameters

list_name

Specifies the name of an Autonomous System (AS) ACL.

Modes

Privileged EXEC mode

Examples

The following example displays AS-path ACL status for a specified list.

```
device# show ip as-path-list myaspathlist
ip as-path access-list foo
   seq 5 deny my_string
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 optional mask.

/prefix
IPv4 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

The following example displays sample output from the **show ip bgp** command.

```
device# show ip bgp
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

Examples

The following example show sample output for the **show ip bgp attribute-entries** command.

```
device# show ip bgp attribute-entries

        Total number of BGP Attribute Entries: 2
1       Next Hop   : 100.1.1.2        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    :100 (length 3)
        AsPathLen: 1  AsNum: 1, SegmentNum: 1, Neighboring As: 100, Source As 100
        AsPath_Addr: 0x12df9e12 Nh_Addr: 0x12e02a26 Nlri_Addr: 0x12e2240c Hash:2817 (0x03000292)
        Links: 0x00000000, 0x00000000
        Reference Counts: 5:0:5, Magic: 3
```

History

Release version	Command history
17s.1.00	This command was introduced.

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            Flp Since        Reuse       Pnlty rIdx dBlk
*d  101.0.99.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.98.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.97.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.96.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.95.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.94.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.93.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.92.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.91.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.90.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.89.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.88.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.87.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.86.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
*d  101.0.85.0/24        12.12.1.2       3   0 :1 :34     0 :29:0      2818  5    0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example displays BGP4 filtered routes.

```
device# show ip bgp filtered-routes 10.11.12.13 prefix-list myprefixlist
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
IPv4 address of a neighbor in dotted-decimal notation.

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 for this command shows all configured parameters for the neighbors. Only parameters with values that differ from default values are shown.

Examples

The following example shows sample output for the show ip bgp neighbors command.

```
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
    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
```

History

Release version	Command history
17s.1.00	This command was introduced.

Release version	Command history
18s.1.00	The command output was modified to display configuration information for BGP graceful shutdown.

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

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example shows flap statistics.

```
device#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following 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 118.113.0.1 last-packet-with-error

 Received Message Length: 19
 BGP Message:
  0xffffffff  0xffffffff  0xffffffff  0xffffffff  0x001304

 BGP Header
  Marker:   0xffffffff  0xffffffff  0xffffffff  0xffffffff
  Message Length: (0x0013) 19
  Message Type: (0x04) KEEPALIVE
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 when the **prefix-filter** keyword is used.

```
device# show ip bgp neighbors 10.5.5.6 received prefix-filter
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 118.113.0.1 received-routes

       There are 106 received routes from neighbor 118.113.0.1
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      101.34.0.0/24      118.113.0.1      none      100        0      E
         AS_PATH: 118 2
2      102.34.0.0/24      118.113.0.1      none      100        0      E
         AS_PATH: 118 2
3      112.113.114.0/28   118.113.0.1      none      100        0      E
         AS_PATH: 118 2
4      114.4.1.0/31       118.113.0.1      none      100        0      E
         AS_PATH: 118 2
5      114.114.114.114/32 118.113.0.1      none      100        0      E
         AS_PATH: 118 2
6      118.114.0.0/31     118.113.0.1      none      100        0      E
         AS_PATH: 118 2
7      119.219.32.0/20    118.113.0.1     1          100        0      BE
         AS_PATH: 118
8      119.219.48.0/20    118.113.0.1     1          100        0      BE
         AS_PATH: 118
9      119.219.64.0/20    118.113.0.1     1          100        0      BE
         AS_PATH: 118
10     119.219.80.0/20    118.113.0.1     1          100        0      BE
         AS_PATH: 118
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

mask

IP mask of the destination network in CIDR notation.

vrf *vrf-name*

Specifies a VRF instance.

detail

Displays detailed RIB route information.

Modes

Privileged EXEC mode

Examples

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

detail
Specifies detailed information.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays sample output for the s**how ip bgp neighbors routes** command when the **best** keyword is used.

```
device# show ip bgp neighbors 10.11.12.13 routes best
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 the defaults are listed.

Examples

The following example shows sample output from the **show ip bgp peer-group** command.

```
device# show ip bgp peer-group

1   BGP peer-group is pg_vrf10, Remote AS: 4001183001
    Description: bgp_vrf4@-4001183001
       MD5 Password: $MiJTfXJVRzMxTTNRUVpaVzhRUVo=
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members.

2   BGP peer-group is pg_vrf11, Remote AS: 4001183011
    Description: bgp_vrf4@-4001183011
       MD5 Password: $MiJTfXJVRzMxTTNRUVpaVzhRWlo=
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members.
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** | **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.

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 input from the **show ip bgp routes** command when an IP address is specified.

```
device# show ip bgp routes  50.55.55.10

Number of BGP Routes matching display condition : 8
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      10.55.55.0/24      16.1.1.1         0         100        0      BME
         AS_PATH: 65200 65100
2      10.55.55.0/24      17.1.1.1         0         100        0      ME
         AS_PATH: 65200 65100
3      10.55.55.0/24      19.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
4      10.55.55.0/24      21.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
5      10.55.55.0/24      18.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
6      10.55.55.0/24      22.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
7      10.55.55.0/24      23.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
8      10.55.55.0/24      20.1.1.1         0         100        0      mE
         AS_PATH: 65200 65100
       Last update to IP routing table: 0h28m14s       Route is advertised to 7 peers:
        17.1.1.1(65200)                          18.1.1.1(65200)
19.1.1.1(65200)
        20.1.1.1(65200)                          21.1.1.1(65200)
22.1.1.1(65200)
        23.1.1.1(65200)
```

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example displays summary BGP information.

```
device# show ip bgp summary

BGP4 Summary
  Router ID: 4.4.4.4   Local AS Number: 65300
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 2
  Number of Neighbors Configured: 8, UP: 8
  Number of Routes Installed: 80088, Uses 7688448 bytes
  Number of Routes Advertising to All Neighbors: 70077 (10011 entries), Uses 600660 bytes
  Number of Attribute Entries Installed: 16, Uses 1664 bytes
  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
…
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip community-list

Displays the status of community lists.

Syntax

show ip community-list *list_name*

Parameters

list_name

Specifies a BGP community list.

Modes

Privileged EXEC mode

Examples

The following example displays information for a specified list.

```
device# show ip community-list

ip community-list standard commStd
   seq 10 permit 0:12345
   seq 15 permit 111:222
   seq 20 permit 65283:65535 0:0

 ip community-list extended extcommlist
   seq 5 deny myExpression
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip dhcp relay address interface

Displays IP DHCP relay addresses configured on supported interfaces.

Syntax

show ip dhcp relay address interface [**ethernet** *slot/port*| **ve** *interface number*]

Parameters

ethernet*slot/port*
Interface name in slot/port format.

ve*interface number*
Interface name in slot/port format.

Modes

Privileged EXEC mode

Examples

The following example displays DHCP relay address(es) configured on interface 0/4:

```
device# show ip dhcp relay address interface ethernet 0/4
---------                    -------------                    --------
Interface                    Relay Address                    VRF Name
---------                    -------------                    --------
Eth 0/4                       10.3.4.5                         blue
Eth 0/4                       10.5.1.1                         default-vrf
```

The following example displays DHCP relay address(es) configured on Ve 300:

```
device# show ip dhcp rel add int ve 300

---------                  -------------                    --------
Interface                  Relay Address                    VRF Name
---------                  -------------                    --------
Ve 300                        10.0.1.2                       default-vrf
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip dhcp relay statistics

Displays the general information about the DHCP Relay function.

Syntax

show ip dhcp relay staistics

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 switch. As a result, the DHCP renewal Request/ACK and DHCP Release packets are not 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **client** *clientID* | **cluster** *clusterID*]

Parameters

detail
Displays detailed information.

interface
Specifies an interface type.

vlan *vlan-id*
Specifies a VLAN interface.

client *clientID*
Specifies a Multi-Chassis Trunk (MCT) client.

cluster *clusterID*
Specifies an MCT cluster.

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: 1
IGMP Connected Group Membership
Group Address    Interface           Uptime      Expires    Last Reporter     Version
225.1.1.1        vlan300             00:00:03    Never      Static            2
  Member Ports:  eth0/32
```

The following example displays the IP IGMP groups detail.

```
device# show ip igmp groups detail
Group : 225.1.1.1
        Interface        vlan300
        Uptime           00:02:49
        Expires:         Never
        Last Reporter:   Static
        Member Ports:    eth0/32
        Last Reporter Mode: 2
                INCL_SRC_LIST: Nil
                EXCL_SRC_LIST: Nil
```

The following example displays the IP IGMP routes learned over an MCT cluster.

```
device# show ip igmp groups cluster 1

Total Number of IGMP routes: 500
IGMP Connected Group Membership
Group Address    Source Address    Interface    Member    Type    Filter Mode    Mcast DF    Peer
Address
-------------------------------------------------------------------------------------------------
-
227.0.0.1        Nil               Vlan 150     ICL        CEP    EXCLUDE        -
2.2.2.10
227.0.0.2        Nil               Vlan 150     ICL        CEP    EXCLUDE        -
2.2.2.10
227.0.0.3        Nil               Vlan 150     ICL        CEP    EXCLUDE        -
2.2.2.10
228.0.0.1        Nil               Vlan 150     Po 6       CCEP   EXCLUDE        DF
2.2.2.10
228.0.0.2        Nil               Vlan 150     Po 6       CCEP   EXCLUDE        DF
2.2.2.10
228.0.0.3        Nil               Vlan 150     Po 6       CCEP   EXCLUDE        Non-DF
2.2.2.10
228.0.0.5        Nil               Vlan 150     Po 6       CCEP   EXCLUDE        Non-DF
2.2.2.10
228.0.1.6        Nil               Vlan 150     Po 6       CCEP   EXCLUDE        Non-DF
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.01	Support for MCT cluster and client was added.

show ip igmp snooping

Displays IGMP snooping information.

Syntax

show ip igmp snooping [**mrouter vlan** *vlan_id* | **vlan** *vlan_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.

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 45
Vlan ID: 45
 Multicast Router ports:  eth3/2
 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:  eth4/22 eth6/15
  Mapped MAC address: 0100.5e00.0001
```

The following example displays IGMP snooping Mrouter information.

```
device# show ip igmp snooping mrouter
Vlan     Interface    Expires (Sec)
300      eth0/3       184
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip igmp static-groups

Displays information about the Internet Group Management Protocol (IGMP) static groups.

Syntax

show ip igmp static-groups [**detail** | **interface** *ethernet / port-channel / ve* | **vlan***vlan-id*]

Parameters

detail

Displays detailed information about the IP IGMP static groups.

interface*ethernet / port-channel / ve*

Specifies the interface type.

vlan *vlan-id*

Specifies the VLAN-ID.

Modes

Privileged EXEC mode

Command Output

The **show ip igmp static groups** command displays the following information:

Output field	Description
Group address	The IP address of the IGMP group.
Interface	The name of the interface.
Uptime	The amount of time the group membership has been up.
Expires	The time by which the group membership expires.
Last Reporter	The most recent source that has joined the multicast group.

Examples

The following example displays information about the IP IGMP static groups.

```
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address    Interface            Uptime      Expires    Last Reporter     Version
226.1.1.1        vlan100              00:00:14    Never      Static            2
  Member Ports:  eth0/3
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

IGMP Error Statistics:
Unknown types            0
Bad Length               0
Bad Checksum             0
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip interface

Displays the IP address, status, and configuration for a specified interface.

Syntax

show ip interface { **brief** | **ethernet** *slot/port* | **loopback** *number* | **port-channel** *port-number* | **ve** *vlan-id* }

Parameters

brief
Specifies a brief summary of IP interface status and configuration.

ethernet *slot/port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback interface. Valid values range from 1 through 255.

port-channel *port-number*
Specifies a port channel interface. Valid values range from 1 through 1024.

ve *vlan-id*
Specifies a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Usage Guidelines

You can also display a brief summary of such information for all interfaces.

Examples

The following example displays information about all of the interfaces in the summary format.

```
device# show ip interface brief

Interface         IP-Address      Vrf             Status                  Protocol
==========        ==========      =============   ====================    ========
Port-channel 1    unassigned                      administratively down   down
Port-channel 2    unassigned                      administratively down   down
Port-channel 7    unassigned                      up                      up
Loopback 1        1.2.3.4         default-vrf     up                      up
Ethernet 0/1      unassigned      default-vrf     administratively down   down
Ethernet 0/2      unassigned      default-vrf     up                      up
Ve 7              19.19.19.1      default-vrf     up                      up
```

The following example displays the IP interface status of a specified Ethernet port.

```
device# show ip interface ethernet 0/1
 Ethernet 0/1 is up protocol is up
 Primary Internet Address is 10.0.0.4/24 broadcast is 10.0.0.255
 IP MTU is 1500
 Proxy Arp is Enabled
 ICMP unreachables are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 Vrf : default-vrf
```

The following example displays the IP interface status of a loopback interface.

```
device# show ip interface loopback 1
 Loopback 1 is up protocol is up
 Primary Internet Address is 1.2.3.4/32
 IP MTU is 1500
 Proxy Arp is not Enabled
 ICMP unreachables are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 Vrf : default-vrf
```

The following example displays the IP interface status of a VE interface.

```
device# show ip int ve 10
 Ve 10 is up protocol is down
 Vlan is 10
 Hardware is Virtual Ethernet, address is 609c.9f00.2e87
     Current address is 609c.9f00.2e87
 Interface index (ifindex) is 1207959562
 Primary Internet Address is 100.0.0.1/24 broadcast is 100.0.0.255
 IP MTU is 1500
 Proxy Arp is Enabled
 Vrf : default-vrf
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip interface brief

Display the status of IP interfaces.

Syntax

show ip interface brief

Modes

Privileged EXEC mode

Examples

The following is sample output.

```
device# show ip interface brief
Flags:  I - Insight Enabled
Interface            IP-Address       Vrf                  Status                   Protocol
==================   ==========       ==================   ======================   ========
Port-channel 20(I)   unassigned                            up                       up
Ethernet 0/1         unassigned       default-vrf          administratively down    down
Ethernet 0/2         unassigned       default-vrf          administratively down    down
...
```

The following Network Packet Broker (NPB) output indicates interfaces and port-channels configured for internal loopback.

```
device# show ip interface brief
Flags:  U - Unnumbered interface, I - Insight Enabled, L - Internal Loopback
Interface           IP-Address  Vrf          Status                 Protocol
==============      ==========  ==========   ====================   ========
Port-channel 10(L)  unassigned               up                     up
Ethernet 0/1        unassigned  default-vrf  administratively down  down
Ethernet 0/2        unassigned  default-vrf  administratively down  down
Ethernet 0/3        unassigned  default-vrf  administratively down  down
Ethernet 0/4        unassigned  default-vrf  administratively down  down
Ethernet 0/5(L)     unassigned  default-vrf  up                     up
Ethernet 0/6(L)     unassigned  default-vrf  up                     up
```

History

Release version	Command history
17s.1.01	This command was introduced.
18s.1.01	The command was modified to support the NPB **loopback phy** option.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip ospf border-routers

Displays information about area border routers (ABRs) and autonomous system boundary routers (ASBRs).

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

Examples

The following example displays information for all ABRs and ASBRs.

```
device# show ip ospf border-routers
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Examples

The following example shows sample output from the show ip ospf config command.

```
device# show ip ospf config
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **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. The specified slot must be 0 if the switch does not contain slots.

loopback *number*
Specifies a loopback port number. Valid values range from 1 through 255.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096

Modes

Privileged EXEC mode

Examples

The following example displays OSPF information about all enabled interfaces.

```
device# show ip ospf interface

Ethernet 0/2 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: -
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip ospf neighbor

Displays OSPF neighbor information.

Syntax

show ip ospf neighbor [**extensive**] [**ethernet** *slot/port* | **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. The specified slot must be 0 if the switch does not contain slots.

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

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 0/2        53.1.1.36       1   FULL/DR    53.1.1.1        200.1.2.3       6       66  0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Examples

The following example shows sample output for the **show ip ospf redistribute route** command.

```
device# show ip ospf redistribute route
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Examples

The following example displays all OSPF-calculated routes.

```
device# show ip ospf routes

OSPF Regular Routes 7:

      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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip ospf summary

Displays summary information for all OSPF instances.

Syntax

show ip ospf summary [**vrf** *vrfname*]

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.

Modes

Privileged EXEC mode

Examples

```
device# show ip ospf summary

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     5       2       1         12      2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The specified slot must be 0 if the switch does not contain slots.

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

Examples

The following example displays 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!
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip ospf virtual link

Displays information about virtual links.

Syntax

show ip ospf virtual link [*index*] [**vrf** *vrfname*]

Parameters

index

Shows information about a specified virtual link.

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

Examples

The following example shows information about all virtual links.

```
device# show ip ospf virtual link
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip ospf virtual neighbor

Displays information about virtual neighbors.

Syntax

show ip ospf virtual neighbor [*index*] [**vrf** *vrfname*]

Parameters

index

Shows information about a specified virtual neighbor.

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

Examples

The following example shows information about all virtual neighbors.

```
device# show ip ospf virtual neighbor
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ip prefix-list

Displays the status of an IPv4 prefix list.

Syntax

show ip prefix-list *name*

Parameters

name

Name of an IPv4 prefix list.

Modes

Privileged EXEC mode

Examples

To display the status of the IPv4 prefix list "mylist":

```
device# show ip prefix-list
ip extcommunity-list standard 1
   seq 10 permit  rt 200:200

 ip extcommunity-list standard 10
   seq 10 permit   soo 4.3.2.1:987
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 connected [**vrf** *vrf-name*]

show ip route import [*src-vrf-name*] [**vrf** *vrf-name*]

show ip route nexthop [*nexthopID* [**ref-routes**]] [**vrf** *vrf-name*]

show ip route ospf [**vrf** *vrf-name*]

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 prefix.

all
Specifies information for all configured IPv4 routes.

bgp
Specifies BGP route information.

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.

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.

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

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. Sample 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 10.20.232.1, mgmt 1, [1/1], 11d23h, static, tag 0
10.20.232.0/21, attached
    *via DIRECT, mgmt 1, [0/0], 11d23h, direct, tag 0
10.20.234.119/32, attached
    *via DIRECT, mgmt 1, [0/0], 11d23h, local, tag 0
```

Examples

The following example displays sample output from the **show ip route** command.

```
device# show ip route
IP Routing Table for VRF "default-vrf"
Total number of IP routes: 21
'[x/y]' denotes [preference/metric]

2.4.0.2/31
     via 2.6.0.2, Ve 2603, [20/0], 3m23s, eBgp, tag 0
2.6.0.0/29, attached
     via DIRECT, Ve 2603, [0/0], 27m24s, direct, tag 0
2.6.0.3/32, attached
     via DIRECT, Ve 2603, [0/0], 27m24s, local, tag 0
2.7.0.0/29
     via 2.6.0.2, Ve 2603, [20/0], 27m4s, eBgp, tag 0
```

The following example displays output for the **system-summary** option.

```
device# show ip route system-summary
System Route Count: 27107 Max routes: 65536 (Route limit not exceeded) System Nexthop Count: 1402
Max nexthops: 2048 (Nexthop limit not exceeded)
One Path Nexthop Count: 1662 Max One Path Nexthops: 16384

VRF-Name: default-vrf
  Route count: 0 Max routes: Not Set (Route limit not exceeded)
  0 connected, 0 static, 0 OSPF, 0 BGP

VRF-Name: mgmt-vrf
  Route count: 3 Max routes: Not Set (Route limit not exceeded)
  1 connected, 1 static, 0 OSPF, 0 BGP

VRF-Name: orange
  Route count: 0 Max routes: Not Set (Route limit not exceeded)
  0 connected, 0 static, 0 OSPF, 0 BGP
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.00	• The **system-summary** option was modified to display information about the number of one-path nexthops used in the device and the documentation was updated to include an example of the **show ip route system-summary** command.
18s.1.01	The output for the **show ipv6 route** was updated.

show ip route-map

Displays the status of an IPv4 route map.

Syntax

show ip route-map *namenumber*

Parameters

name

Name of an IPv4 route map.

Modes

Privileged EXEC mode

Examples

The following example shows command output for all ip route-maps configured on the device.

```
device# show ip route-map
route-map primaryMap
  seq 10 permit
    match as-path myAsPath
  seq 22 permit
    continue 50
    match vrf foo1
    set comm-list foo1 delete
  seq 25 permit
    match community foobar
    match extcommunity 22
    match ip address prefix-list foo
    set as-path prepend 100 200 300
  seq 30 permit
    match community foobar exact-match
    set community local-as
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 anycast-gateway

Displays details for IPv6 anycast gateway for all or specified virtual Ethernet (VE) interfaces or VRF instances.

Syntax

show ipv6 anycast-gateway [**interface** *VE* | **vrf** *VRF-name*]

Parameters

interface *VE*

Specifies a VE interface.

vrf *VRF-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

To display details for IPv6 anycast gateway for all VE interfaces:

```
device# show ipv6 anycast gateway
Gateway mac: 000a.000b.000d
interface     ip address            state
ve10          1234:2::22/64         Active
ve10          1234:3::22/64         Active
ve20          1234:33::33/64        Active
```

To display details for IPv6 anycast gateway for a specified VE interface:

```
device# show ipv6 anycast-gateway interface ve 10
Gateway mac: 000a.000b.000d
interface     ip address            state
ve10          1234:2::22/64         Active
ve10          1234:3::22/64         Active
```

History

Release version	Command history
17s.1.01	This command was introduced.

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

The following example displays sample output from the **show ipv6 bgp** command.

```
device# show ipv6 bgp
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Each set of attributes is unique and can be associated with one or more routes. The device typically has fewer attribute entries than routes.

Examples

The following 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   : 1206::2                                MED      :1              Origin:IGP
        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
        AsPath_Addr: 0x12df9d97 Nh_Addr: 0x12e02785 Nlri_Addr: 0x12e2238c Hash:4981 (0x01000000)
        Links: 0x00000000, 0x00000000
        Reference Counts: 1:0:2, Magic: 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example displays BGP4+ filtered routes.

```
device# show ipv6 bgp filtered-routes
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example displays flap statistics.

```
device# show ipv6 bgp flap-statistics
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 bgp neighbors

Displays configuration information and statistics for BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors [*ipv6-addr*]

show ipv6 bgp neighbors last-packet-with-error [**vrf** *vrf-name*]

show ipv6 bgp neighbors routes-summary [**vrf** *vrf-name*]

show ipv6 bgp neighbors vrf *vrf-name*

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

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 defaults are shown.

Examples

The following example shows sample output from the show ipv6 bgp neighbors command.

```
device# show ipv6 bgp neighbors

    Total number of BGP Neighbors: 3
1   IP Address: fd80:3001:4031:1::225, AS: 4031 (EBGP), RouterID: 40.31.1.230, VRF: v3001
    State: ESTABLISHED, Time: 8h17m2s, KeepAliveTime: 30, HoldTime: 90
       KeepAliveTimer Expire in 1 seconds, HoldTimer Expire in 60 seconds
    Minimal Route Advertisement Interval: 0 seconds
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 1       0       1110      0            0
       Received: 1       3       995       0            0
    Last Update Time: NLRI              Withdraw               NLRI                Withdraw
                  Tx: ---               ---                 Rx: 8h17m1s             ---
    Last Connection Reset Reason:User Reset Peer Session
    Notification Sent:     Unspecified
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer Negotiated IPV6 unicast  capability
      Peer configured for IPV6 unicast  Routes
    Neighbor ipv6 MPLS Label Capability Negotiation:
    Neighbor AS4 Capability Negotiation:
      Peer configured for AS4  capability
    Outbound Policy Group:
       ID: 5, Use Count: 7
       Byte Sent:   21143, Received: 0
       Local host:  fd80:3001:4031:1::118, Local  Port: 8084
       Remote host: fd80:3001:4031:1::225, Remote Port: 179
...
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* **advertised-routes** [**detail** | **/** *mask-bits*] [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 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

The following example displays the details of advertised routes.

```
device# show ipv6 bgp neighbors fdcd:3001:3009:1::113 advertised-routes

       There are 6 routes advertised to neighbor fdcd:3001:3009:1::113
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      fd70::/128          fdcd:3001:3009:1::118
                                           none                  0      BE
         AS_PATH: 4001183001 4031
2      fd70::1/128         fdcd:3001:3009:1::118
                                           none                  0      BE
         AS_PATH: 4001183001 4031
3      fd70::2/128         fdcd:3001:3009:1::118
                                           none                  0      BE
         AS_PATH: 4001183001 4031
4      fd70::3/128         fdcd:3001:3009:1::118
                                           none                  0      BE
         AS_PATH: 4001183001 4031
5      fd70::4/128         fdcd:3001:3009:1::118
                                           none                  0      BE
         AS_PATH: 4001183001 4031
6      fd70::5/128         fdcd:3001:3009:1::118
                                           none                  0      BE
         AS_PATH: 4001183001 4031
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* **flap-statistics** [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*
Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 bgp neighbors flap-statistics** command.

```
device# show ipv6 bgp neighbors flap-statistics
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* **last-packet-with-error** [**decode**] [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 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

The following 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 last-packet-with-error

    Total number of BGP Neighbors: 3
1   IP Address: fdcd:3001:3009:1::113
    Last error:
    BGP4: 19 bytes hex dump of packet that contains error
    ffffffff ffffffff ffffffff ffffffff 00130404
2   IP Address: fdcd:3001:3009:1::114
    Last error:
    BGP4: 19 bytes hex dump of packet that contains error
    ffffffff ffffffff ffffffff ffffffff 00130404
…
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **received**

show ipv6 bgp neighbors *ipv6-addr* **received detail** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **received prefix-filter** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* **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

The following example displays sample output for the **show ipv6 bgp neighbors received-routes** command.

```
device# show ipv6 bgp neighbors fd80:3001:4031:1::225 received-routes

       There are 6 received routes from neighbor fd80:3001:4031:1::225
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      fd70::/128         fd80:3001:4031:1::225
                                          none       100        0      BE
         AS_PATH: 4031
2      fd70::1/128        fd80:3001:4031:1::225
                                          none       100        0      BE
         AS_PATH: 4031
3      fd70::2/128        fd80:3001:4031:1::225
                                          none       100        0      BE
         AS_PATH: 4031
4      fd70::3/128        fd80:3001:4031:1::225
                                          none       100        0      BE
         AS_PATH: 4031
5      fd70::4/128        fd80:3001:4031:1::225
                                          none       100        0      BE
         AS_PATH: 4031
6      fd70::5/128        fd80:3001:4031:1::225
                                          none       100        0      BE
         AS_PATH: 4031
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 bgp neighbors rib-out-routes

Displays information about BGP4+ outbound RIB routes.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes** *ipv6-addr mask* [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes detail** *ipv6-addr mask* [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes detail** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 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

The following example shows sample output from the **show ipv6 bgp neighbors rib-out-routes** command.

```
device# show ipv6 bgp neighbors fdcd:3001:3009:1::113 rib-out-routes vrf v3001

       There are 200 RIB_out routes for neighbor fdcd:3001:3009:1::113
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      fd70::/128          fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 4031
2      fd70::1/128         fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 40
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* **routes** [**vrf** *vrf-name*]

show ipv6 bgp neighbors *ipv6-addr* **routes** [**best** | **not-installed-best** | **unreachable** [**vrf** *vrf-name*]]

show ipv6 bgp neighbors *ipv6-addr* **routes detail** [**best** | **not-installed-best** | **unreachable** [**vrf** *vrf-name*]]

show ipv6 bgp neighbors *ipv6-addr* **routes detail** [**vrf** *vrf-name*]

Parameters

ipv6-addr
IPv6 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

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4+ neighbors.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **routes-summary** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Command 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).
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.

Output field	Description
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.
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

The following example shows sample output from the **show ipv6 bgp neighbors routes-summary** command.

```
device# show ipv6 bgp neighbors routes-summary
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example shows sample output from the **show ipv6 bgp peer-group** command.

```
device# show ipv6 bgp peer-group

1   BGP peer-group is pg_vrf11, Remote AS: 4001143011
    Description: bgp_vrf4@-4001183011
       MD5 Password: $MiJTfXJVRzMxTTNRUVpaVzhRWlo=
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members.

2   BGP peer-group is pg_vrf12, Remote AS: 4001143021
    Description: bgp_vrf4@-4001183021
       MD5 Password: $MiJTfXJVRzMxTTNRUVpaVzhRfFo=
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members.
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example shows sample input from the **show ipv6 bgp routes** command.

```
device# show ipv6 bgp routes

Total number of BGP 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
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      fd70::/128          fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 4031
2      fd70::1/128         fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 4031
3      fd70::2/128         fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 4031
4      fd70::3/128         fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 4031
5      fd70::4/128         fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 4031
6      fd70::5/128         fd80:3001:4031:1::225
                                           none       100        0      BE
         AS_PATH: 4031
```

The following 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       : 200
  Distinct BGP destination networks                  : 200
  Filtered bgp routes for soft reconfig              : 0
  Routes originated by this router                   : 0
  Routes selected as BEST routes                     : 200
  Routes Installed as BEST routes                    : 200
  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                : 200
  BEST routes not valid for IP forwarding table      : 0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example displays summary BGP4+ information.

```
device# show ipv6 bgp summary

  BGP4 Summary
  Router ID: 30.1.1.8   Local AS Number: 4001183001
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 3, UP: 3
  Number of Routes Installed: 200, Uses 19200 bytes
  Number of Routes Advertising to All Neighbors: 400 (200 entries), Uses 12000 bytes
  Number of Attribute Entries Installed: 1, Uses 104 bytes
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  fd80:3001:4031:1::225
                    4031        ESTAB     8h12m 5s    200      0        0        0
  fdcd:3001:3009:1::113
                    4001133001  ESTAB     8h 6m47s    0        0        200      0
  fdcd:3001:3009:1::114
                    4001143001  ESTAB     6h40m33s    0        0        200      0
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 counters interface

Displays ipv6 statistics for an interface.

Syntax

show ipv6 counters interface [**ethernet** *slot/plot* | **loopback** *loopback-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.

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 0/1

 Interface Ethernet 0/1 IPv6 statistics (ifindex 406896641)
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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 address(es) configured per interface.

```
device# show ipv6 dhcp relay address interface ethernet 0/4

Interface              Relay Address                        VRF Name             Outgoing Interface
---------              -------------                        -------------        ----------------
Eth 0/4              4001::101                            default-vrf
Eth 0/4              fe80::8                                blue                         Ve 100
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 dhcp relay statistics

Displays general information about the DHCPv6 Relay function.

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

To display statistics for the device:

```
device# show ipv6 dhcp relay statistics

Packets dropped           :  0
    Error                 :  0
Packets received          :  0
    SOLICIT               :  0
    REQUEST               :  0
    CONFIRM               :  0
    RENEW                 :  0
    REBIND                :  0
    RELEASE               :  0
    DECLINE               :  0
    INFORMATION-REQUEST   :  0
    RELAY-FORWARD         :  0
    RELAY-REPLY           :  0
Packets sent              :  0
    RELAY-FORWARD         :  0
    REPLY                 :  0
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 interface

Displays details of IPv6 interfaces.

Syntax

show ipv6 interface [**brief** | **ethernet** *slot/port* | **loopback** loopback-port-number | **ve** *ve_id*]

Parameters

brief

Displays brief interface information.

ethernet

Specifies Ethernet interface.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots

port

Specifies a valid port number.

loopback *loopback-port-number*

Specifies the loopback interface. The range is from 1 to 255.

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 0/25
 Ethernet 0/25 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 mld groups

Displays information about a specific IPv6 MLDv1 group or a VLAN.

Syntax

show ipv6 mld groups [*ipv6 address*] [*vlan-id*] | [**summary**]

Parameters

ipv6 address
Specifies the multicast group address.

vlan-id
Specifies a VLAN ID.

summary
Displays summary information.

Modes

Privileged EXEC mode

Examples

To display information about all IPv6 MLDv1 groups:

```
device# show ipv6 mld groups
```

To display information about an IPv6 MLDv1 group for a specific multicast address:

```
device# show ipv6 mld groups ff1e::1
```

To display information about all IPv6 MLDv1 groups for a VLAN:

```
device# show ipv6 mld groups vlan 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 mld snooping

Displays information about the actively enabled IPv6 MLDv1 snooping mechanism and related configurations such as the active querier, the number of group-learned mrouters present, and other querier details.

Syntax

show ipv6 mld snooping [**vlan** *vlan-id*] [**mrouter**]

Parameters

vlan*vlan-id*

Specifies a VLAN ID.

mrouter

Specifies all multicast router statistics.

Modes

Privileged EXEC mode

Examples

The following example displays the output for the **show ipv6 mld snooping mrouter** command.

```
device# show ipv6 mld snooping mrouter
Vlan     Interface    Expires (Sec)
100      Eth 0/3      Never
```

The following example displays the output for the **show ipv6 mld snooping** command.

```
device# show ipv6 mld snooping

Vlan ID: 100
Multicast Router ports: Eth 0/3
Querier - enabled
 MLD Operation mode: MLDv1
Fast-Leave :Disabled
Max Response time = 10 s
Query interval = 30 s
Last Member Query Interval = 1 s
Last Member Query Count = 2
Startup Query Interval = 7 s
Startup Query Count = 0
Robustness Variable = 2
Restrict Unknown Multicast : Disabled
Number of Multicast Groups: 5

  Group: ff1e::1
  Member Ports: Eth 0/4
```

The following example displays the output for the **show ipv6 mld snooping vlan 100** command.

```
device# show ipv6 mld snooping vlan 100

Vlan ID: 100
Multicast Router ports: Eth 0/3
Querier - enabled
 MLD Operation mode: MLDv1
Fast-Leave :Disabled
Max Response time = 10 s
Query interval = 30 s
Last Member Query Interval = 1 s
Last Member Query Count = 2
Startup Query Interval = 7 s
Startup Query Count = 0
Robustness Variable = 2
Restrict Unknown Multicast : Disabled
Number of Multicast Groups: 5

  Group: ff1e::1
  Member Ports: Eth 0/4
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 mld statistics

Displays IPv6 MLDv1 statistics for a VLAN.

Syntax

show ipv6 mld statistics vlan *vlan-id*

Parameters

vlan*vlan-id*

Specifies the VLAN-ID.

Modes

Privileged EXEC mode

Examples

To display information about IPv6 MLDv1 statistics for a specific VLAN interface:

```
device# show ipv6 mld statistics vlan 100
MLD packet statistics for all interfaces in vlan 100:
MLD Message type      Edge-Received   Edge-Sent   Edge-Rx-Errors
General Query          0                     8             0
Group Specific Query   0                     0             0
V1 Membership Report   45                    0             0
V2 Membership Report   0                     0             0
Group Leave            0                     0             0

MLD Error Statistics:
Checksum Error         0
Size_or_Range_Error    0
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 nd

Displays the router advertisement information.

Syntax

show ipv6 nd

show ipv6 nd interface [**vrf** *vrf-name*]

show ipv6 nd interface { **ethernet** *slot* **/** *port* | **ve** *ve-number* } [**prefix**]

Parameters

interface
Specifies an interface.

vrf *vrf-name*
Specifies a VRF instance.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

ve *ve-number*
Specifies a virtual Ethernet (VE).

prefix
Displays prefix information.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show ipv6 nd** command output for a specified port.

```
device# show ipv6 nd interface ethernet 0/5
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command 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.
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
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 0/41                   00:00:17 L
4006(V) fd80:113:114:1:4006::1002 00ef.4006.3602 Eth 0/41                   00:00:17 L
4006(V) fe80::1                   00ef.4006.3601 Eth 0/41                   00:16:16 L
4006(V) fe80::2                   00ef.4006.3602 Eth 0/41                   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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Command 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.
Proxy Nd	Displays the number of packets for which the device has sent proxy-Nd 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    Proxy Nd
-----------------------------------------------------------
110 (V)         0             117           0
254 (V)         3             10            0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Command 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 neighbor

Displays the IPv6 neighbors.

Syntax

show ipv6 neighbor [*ipv6-address*] [**vrf** *vrf-name*]

show ipv6 neighbor [**dynamic** | **static**] [**summary**] [**vrf** *vrf-name*]

show ipv6 neighbor [**ethernet** *slot* **/** *port* | **ve** *ve-num*] [**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
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number. Must be `0` if the switch does not contain slots.

port
Specifies a valid port number.

static
Displays the static IPv6 neighbors.

dynamic
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

Examples

The following example is output of the **show ipv6 neighbor summary** command.

```
device# show ipv6 neighbor summary
No of Total Entries   No of Static Entries  No of Dynamic Entries
-------------------------------------------------------------------
2003                  0                     2003
```

The following example is output of the **show ipv6 neighbor dynamic vrf** command.

```
device# show ipv6 neighbor dynamic vrf vrf-1
Address         Mac-address    Interface     MacResolved         Age          Type
-------------------------------------------------------------------------------
2001::10    0010.9400.0066     0/2             yes           00:00:13    Dynamic
2001::11    0010.9400.0067     0/2             yes           00:00:13    Dynamic
2001::12    0010.9400.0068     0/2             yes           00:00:13    Dynamic
2001::13    0010.9400.0069     0/2             yes           00:00:13    Dynamic
2001::14    0010.9400.006a     0/2             yes           00:00:13    Dynamic
2001::15    0010.9400.006b     0/2             yes           00:00:13    Dynamic
2001::16    0010.9400.006c     0/2             yes           00:00:13    Dynamic
2001::17    0010.9400.006d     0/2             yes           00:00:13    Dynamic
2001::18    0010.9400.006e     0/2             yes           00:00:13    Dynamic
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 ospf

Displays OSPFv3 information.

Syntax

show ipv6 ospf [**vrf** *name*]

Parameters

vrf *name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the show ipv6 ospf command.

```
device# show ipv6 ospf

 OSPFv3 Process number 0 with Router ID 0x01010101(1.1.1.1)
 Running 0 days 0 hours 0 minutes 40 seconds
 Number of AS scoped LSAs is 0
 Sum of AS scoped LSAs Checksum is 00000000
 External LSA Limit is 250000
 Database Overflow Interval is 10
 Database Overflow State is NOT OVERFLOWED
 Route calculation executed 3 times
 Pending outgoing LSA count 2
 Authentication key rollover interval 300 seconds
 Number of areas in this router is 1
 High Priority Message Queue Full count: 0
 BFD is disabled, BFD HoldoverInterval: 0
 Graceful restart helper is enabled, strict lsa checking is disabled
 Nonstop Routing is enabled
 Administrative Distance
 - External Routes: 110
 - Intra Area Routes: 110
 - Inter Area Routes: 110
 Maximum Paths: 8
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

```
device# show ipv6 ospf area
Area 0:
  Authentication: Not Configured
  Active interface(s)attached to this area: Ve 200
  Inactive interface(s)attached to this area: None
  Number of Area scoped LSAs is 4
  Sum of Area LSAs Checksum is 0004a7a5
  Statistics of Area 0:
    SPF algorithm executed 4 times
    SPF last updated: 76 sec ago
    Current SPF node count: 3
      Router: 2 Network: 1
      Maximum of Hop count to nodes: 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 databas** command.

```
device# show ipv6 ospf database

LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix Grc:Grace


Area ID         Type LSID       Adv Rtr         Seq(Hex) Age  Cksum Len   Sync
0               Link 6472       1.1.1.1         80000001 371  93e1  56    Yes
0               Link 6416       2.2.2.2         80000001 382  d73d  56    Yes
0               Rtr  0          2.2.2.2         80000003 341  bdfc  40    Yes
0               Rtr  0          1.1.1.1         80000002 341  f096  40    Yes
0               Net  6416       2.2.2.2         80000001 341  b536  32    Yes
0               Iap  192480     2.2.2.2         80000001 341  d8bf  44    Yes
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **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. The specified slot must be 0 if the switch does not contain slots.

loopback *number*

Specifies a loopback port number. Valid values range from 1 through 255.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf interface** command the **brief** keyword is used.

```
device# show ipv6 ospf interface brief

Interface     Area            Status Type Cost  State    Nbrs(F/C)
Ve 200        0               up     BCST 1     BDR      1/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Examples

The following is sample output from the **show ipv6 ospf memory** command.

```
device# show ipv6 ospf memory
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **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
Specifies detailed neighbor information.

interface
Displays OSPFv3 interface information.

ethernet *slot/port*
Specifies an Ethernet slot and port. The specified slot must be 0 if the switch does not contain slots.

loopback *number*
Specifies a loopback port number. Valid values range from 1 through 255.

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]
2.2.2.2           1 Full     2.2.2.2         1.1.1.1         Ve 200        [BDR]
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

  Current Route count: 1
    Intra: 1 Inter: 0 External: 0 (Type1 0/Type2 0)
    Equal-cost multi-path: 0
    OSPF Type: IA- Intra, OA - Inter, E1 - External Type1, E2 - External Type2
   Destination                   Cost       E2Cost     Tag        Flags    Dis
IA 2001::/64                     1          0          0          00000003 110
   Next_Hop_Router               Outgoing_Interface Adv_Router
   ::                            Ve 200             2.2.2.2
```

The following example displays information about a specified OSPFv3 route.

```
device# show ipv6 ospf routes  2001::/64

   Destination                   Cost       E2Cost     Tag        Flags    Dis
IA 2001::/64                     1          0          0          00000003 110
   Next_Hop_Router               Outgoing_Interface Adv_Router
   ::                            Ve 200             2.2.2.2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 **tree** keyword is used.

```
device# show ipv6 ospf spf tree

 SPF tree for Area 0
 +- 1.1.1.1 cost 0
     +- 2.2.2.2:6416(N) cost 1
         +- 2.2.2.2:0 cost 1
```

The following example shows sample output from the **show ipv6 ospf spf** command when the **table** keyword is used.

```
device# show ipv6 ospf spf table

 SPF table for Area 0
  Destination           Bits Options  Cost  Nexthop                    Interface
R 2.2.2.2               ----- V6E---R--    1  fe80::629c:9fff:fe5b:801  Ve 200
N 2.2.2.2[6416]         ----- V6E---R--    1  ::                         Ve 200
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 ospf summary

Displays summary information for all OSPFv3 instances.

Syntax

show ipv6 ospf summary [**all-vrfs** | **vrf** *vrfname*]

Parameters

all-vrfs
Specifies all VRF instances.

vrf *vrfname*
Specifies a non-default VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 ospf summary** command when no arguments or keywords are used.

```
device# show ipv6 ospf summary

Total number of IPv6 OSPF instances: 1

Seq Instance                        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf                     1       1       1         6       1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

User 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.

Command 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ipv6 route

Displays IPv6 router advertisement information.

Syntax

show ipv6 route [**all** | **bgp** | **connected** | **import** *source-name* | **nexthop** *nexthop-id* [**ref-routes**] | **ospf** | **static**] [**vrf** *vrf-name*]

show ipv6 route [**summary** [**vrf** *vrf-name*] | **system-summary**]

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.

nexthop *nexthop-id*
Displays the route nexthop table.

ospf
Specifies OSPF routes.

ref-routes
Displays information for routes matching the next-hop ID.

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.

Modes

Privileged EXEC mode

Examples

The following is an example of **show ipv6 route** command output.

```
device# show ipv6 route
IPv6 Routing Table for VRF "default-vrf"
Total number of IPv6 routes: 22
'[x/y]' denotes [preference/metric]
2:4::/64
     via 2:6::2, Ve 2603, [20/0], 3m13s, eBgp, tag 0
2:6::/64, attached
     via ::, Ve 2603, [0/0], 27m15s, direct, tag 0
2:6::3/128, attached
     via ::, Ve 2603, [0/0], 27m15s, local, tag 0
```

The following is an example of **show ipv6 route system-summary** command output.

```
device# show ip route system-summary
System Route Count: 27107 Max routes: 65536 (Route limit not exceeded) System Nexthop Count: 1402
Max nexthops: 2048 (Nexthop limit not exceeded) One Path Nexthop Count: 1662 Max One Path Nexthops:
16384
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.00	The output for **system-summary** was added.
18s.1.01	The output for the **show ipv6 route** was updated.

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 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)
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* } [**detail** | **summary**]

show ipv6 vrrp interface 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. The slot number must be 0 if the switch does not contain slots.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

Show J through Show Z

show lacp

Displays the Link Aggregation Control Protocol (LACP) traffic statistics for a specific port-channel or for all port-channels; or displays the system ID.

Syntax

show lacp { **counter** [*port-channel*] | **sys-id** }

Parameters

counters

Displays LACP statistics for all port-channel interfaces.

port-channel

Displays counters for a specific port channel interface. Valid values range from 1 through 1024.

sys-id

Displays the 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show license

Displays license information.

Syntax

show license [**eula** | **id**]

Command Default

Displays the licenses installed on the local switch.

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: Mon Dec  5 13:35:00 2016
```

The following example displays the switch license ID:

```
device# show license id
Location  License ID

==================================================

Chassis  10:00:C4:F5:7C:40:01:46
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.02c	Rebranded from Brocade to Extreme.

show link-fault-signaling

Displays the global and interface link-fault signaling (LFS) statuses.

Syntax

show link-fault-signaling

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported both in default system mode and network packet broker (NPB) mode.

Because you cannot override the egress LFS setting, the global and interface "TX" values are always "ON". If there is an egress link fault, the affected interface is always brought down.

Command Output

The **show link-fault-signaling** command displays the following information:

Output field	Description
Global Link Fault	Displays "RX ON" or "RX OFF" and "TX ON".
PORT #	Displays the ethernet or port-channel interface.
LINK FAULT	Displays "RX ON" or "RX OFF" and "TX ON". "(local)" indicates an interface-level LFS configuration.

Examples

The following example displays sample results of the command.

```
device#  show link-fault-signaling
Global Link Fault: RX ON, TX ON
PORT #:       LINK FAULT:
PORT eth0/1:  RX ON, TX ON
PORT eth0/2:  RX OFF, TX ON (local)
PORT eth0/3:  RX ON, TX ON
PORT eth0/4:  RX ON, TX ON
PORT eth0/5:  RX ON, TX ON
PORT eth0/6:  RX ON, TX ON

(output
               truncated)
```

History

Release version	Command history
17s.1.01	This command was introduced.

show link-fault-signaling counters

Displays link-fault signaling (LFS) counter information.

Syntax

show link-fault-signaling counters

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported both in default system mode and network packet broker (NPB) mode.

Command Output

The **show link-fault-signaling counters** command displays the following information:

Output field	Description
Port	Displays the ethernet or port-channel interface.
Local-Fault-Count	Displays the local link-fault counter.
Time-Last-Local-Fault-Detected	Displays the time the most recent local link-fault was detected.
Remote-Fault-Count	Displays the remote link-fault counter.
Time-Last-Remote-Fault-Detected	Displays the time the most recent remote link-fault was detected.

Examples

The following example displays sample results of the command.

```
device#  show link-fault-signaling counters
Port  Local-Fault-  Time-Last-Local-     Remote-Fault-  Time-Last-Remote-
      Count         Fault-Detected       Count          Fault-Detected
====  ============  ==================  =============  ==================
0/1   100           2017-07-17/09:08:03  1000           2017-07-17/09:08:03
0/2   300           2017-07-17/09:08:03  3000           2017-07-17/09:08:03
0/4   500           2017-07-17/09:08:03  5000           2017-07-17/09:08:03
(output
               truncated)
```

History

Release version	Command history
17s.1.02	This command was introduced.

show lldp

Displays Link Layer Discovery Protocol (LLDP) status information.

Syntax

show lldp

Modes

Privileged EXEC mode

Examples

The following example shows how to display LLDP configuration information.

```
device# show lldp

LLDP Global Information
  system-name: SLX
  system-description: Brocade BR-SLX9140 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
  DCBx iSCSI Priority Values: none
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

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 the LLDP interface information for a specified ethernet interface, enter the following:

```
device# show lldp interface ethernet 0/1
LLDP information for Eth 0/1
  State:                   Enabled
  Mode:                    Receive/Transmit
  Advertise Transmitted:   30 seconds
  Hold time for advertise: 120 seconds
  Tx Delay Timer:          1 seconds
  DCBX Version :           pre-CEE
  Auto-Sense :             No
  Transmit TLVs:           Chassis ID              Port ID
                           TTL                     Port Description
                           System Name             IEEE DCBx
  DCBx iSCSI Priority Values: none
```

History

Release version	Command history
17s.1.00	This command was introduced.

show lldp neighbors

Displays Link Layer Discovery Protocol (LLDP) 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

Causes 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 0/18

Local Port  Dead Interval  Remaining Life  Remote Port ID   Remote Port Descr Chassis ID       Tx  Rx
System Name
Eth 0/18      120            115             Ethernet 0/25    Eth 0/25        768e.f807.6000   655 654
R6
```

The following example shows how to display 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: R6
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show mac-address-table

Displays MAC address table information.

Syntax

show mac-address-table

show mac-address-table bridge-domain [*id*]

show mac-address-table cluster *cluster-ID* [{ **client** *client-ID* [**local** | **remote**] } | local | **remote** | { **vlan** *vlan-ID* [**client** *client-ID*] }]

show mac-address-table count [**bridge-domain** *id*]

show mac-address-table [**address** *mac-address*] [**aging-time**] | [**dynamic** [**address** *mac-address*] | [**interface ethernet***0/port* | **port-channel** *interface number*] | **vlan** *vlan id*]] [**interface ethernet***0/port* | **port-channel** *number*] [**mdb** [*mac-address*] | **client** <*client-name*> | **vlan** <*vlan-id*>]] [**static** [**address** *mac-address*] | [**interface ethernet***0/port* | **port-channel** *number*] | [**vlan***vlan id*]] [**vlan***vlan id*]

Parameters

bridge-domain *id*
Specifies displaying information about MAC addresses learned under a bridge domain. When a bridge domain identifier is not specified, information is displayed about MAC addresses learned under all bridge domains.

cluster *cluster-ID*
Specifies the MCT cluster ID.

client *client-ID*
Specifies the client ID.

local
Displays the local MAC addresses for the cluster or the specified client ID.

remote
Displays the remote MAC addresses for the cluster or the specified client ID.

vlan *vlan-ID*
Specifies the VLAN ID.

address *MAC-address*
Displays forwarding information for a 48-bit MAC address. The valid format is *H.H.H* (available in Privileged EXEC mode only).

aging-time
Displays aging-time.

dynamic address *MAC-address*
Specifies the dynamic MAC addresses for an ethernet interface, port-channel, or VLAN. The valid format is *H.H.H* (available in Privileged EXEC mode only).

interface ethernet *0/port*
Specifies the ethernet interface with a valid port number.

interface port-channel *number*
Specifies the port channel interface number. The range is from 1 - 1024 based on the platform.

vlan *vlan id*
Specifies the VLAN interface. The VLAN ID range is from 1 - 4090.

tunnel *tunnel id*
Specifies the tunnel interface. The tunnel ID range is from 1 - 100000.

mdb *MAC-address*
Specifies the MDB information for the cluster client specific macs. The valid format is *H.H.H* (available in Privileged EXEC mode only).

client *client-name*
Displays the client instance. Specify the client name with a maximum of 64 characters.

static address *mac-address*
Specifies the static MAC address for an ethernet interface, port-channel, or VLAN. The valid format is *H.H.H* (available in Privileged EXEC mode only).

Modes

Privileged EXEC mode

Usage Guidelines

To display information about MAC addresses learned under all bridge domains, specify the **bridge-domain** option without a bridge-domain identifier.

Command Output

The **show mac-address-table** command displays the following information:

Output field		Description
Bridge domain		
	BD-Id	Bridge domain identifier
	Mac-address	MAC address
	Type	MAC address type (Dynamic or static)
	State	State (Active or Inactive)
	Ports	Ethernet or port-channel interfaces
	LIF	Logical interface
	peer-ip	IP address of a remote VPLS peer

Examples

The following example shows how to display MAC table information for all bridge domains.

```
device# show mac-address-table bridge-domain all

VlanId/BD-Id   Mac-address           Type     State     Ports/LIF/peer-ip
629(B)            0011.2222.5555     Dynamic  Active    eth 0/3.100
629(B)            0011.2222.6666     Dynamic  Inactive  eth 0/1.500
629(B)            0011.2222.1122     Dynamic  Active    10.12.12.12
629(B)            0011.2222.3333     static   Inactive  po 5.700
629(B)            0011.0101.5555     Dynamic  Active    eth 0/2.400

Total MAC addresses : 5
```

The following example shows the number of forwarding entries in the MAC address table for bridge domain 1.

```
device# show mac-address-table count bridge-domain 1

Total MAC addresses : 5
```

The following example displays the MAC address table aging time.

```
device# show mac-address-table aging-time
     MAC Aging-time : 300 seconds
```

The following command displays the MAC address table for an MCT cluster.

```
device# show mac-address-table cluster 1
```

History

Release version	Command history
17s.1.00	This command was introduced.

show mac-address-table endpoint-tracking

Displays authenticated or nonauthenticated MAC addresses that are learned on ports enabled for endpoint tracking.

Syntax

show mac-address-table endpoint-tracking { **authenticated** |**authentication-failed** } [**interface** { **ethernet** *interface* | **port-channel** *number* }]

Parameters

authenticated
Displays authenticated MAC addresses that are learned.

authentication-failed
Displays nonauthenticated MAC addresses that are learned.

interface
Specifies an Ethernet or port-channel interface.

ethernet*interface*
Specifies an Ethernet interface.

port-channel*number*
Specifies a port-channel.

Modes

Privileged EXEC mode

Usage Guidelines

If an interface is not specified, the status for all ports is displayed.

Examples

This example displays all ports where MAC authentication succeeds.

```
device# show mac-address-table endpoint-tracking authenticated
VlanId/BDId  Mac-address     Type      State(R-Radius,F-FailOpen)           Ports
100 (V)      0001.0100.0001  Dynamic   Authenticated(R)                     Eth 0/5
```

This example displays all ports where MAC authentication fails.

```
device# show mac-address-table endpoint-tracking authentication-failed
VlanId/BDId   Mac-address       Type             State      Ports
100 (V)       0001.0100.0001    Dynamic          Pending    Eth 0/5
100 (V)       0001.0100.0002    Dynamic          Failed     Eth 0/5
```

NOTE

"Pending" means that either (a) authentication is in process for the MAC, or (b) the RADIUS server is not reachable.

This example displays a specified port where MAC authentication succeeds.

```
device# show mac-address-table endpoint-tracking authenticated interface ethernet 0/5
VlanId/BDId  Mac-address     Type      State(R-Radius,F-FailOpen)            Ports
100 (V)      0001.0100.0001  Dynamic   Authenticated(R)                      Eth 0/5
```

This example displays a specified port where MAC authentication fails.

```
device# show mac-address-table endpoint-tracking authentication-failed interface ethernet 0/5
VlanId/BDId   Mac-address       Type              State      Ports
100 (V)       0001.0100.0001    Dynamic           Pending    Eth 0/5
100 (V)       0001.0100.0002    Dynamic           Failed     Eth 0/5
```

History

Release version	Command history
18s.1.01a, 18x.1.01	This command was introduced.

show media

Displays the SFP information for all the interfaces present on a switch.

Syntax

show media

Modes

Privileged EXEC mode

Usage Guidelines

The command output will be several pages long.

The TX Power Field in the **show media** command is not supported by the 40-Gbps optics.

Examples

To display all SFP information:

```
device# show media
  Interface      Ethernet 0/1
  Identifier     3    SFP
  Connector      33   Copper Pigtail
  Transceiver           5500080000000000 10_GB/s
  Name           cu
  Encoding       0
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0    (units km)
  Length 9u      0    (units 100 meters)
  Length 50u     0    (units 10 meters)
  Length 62.5u   0    (units 10 meters)
  Length Cu      1    (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     00:05:1e
  Vendor PN      58-0000051-01    (4x10GE QSFP+ to 4 SFP+ copper cable - 1m)
  Vendor Rev     A
  Wavelength     N/A
  Options        0012
  BR Max         0
  BR Min         0
  Serial No      MAM2160400194JC1
  Date Code      160130
  Optical Monitor No
  Temperature    N/A
  Voltage        N/A
  Current        N/A
  TX Power       N/A
  RX Power       N/A
(Output truncated)
```

History

Release version	Command history
17s.1.00	This command was introduced.

show media interface

Displays the SFP information for an Ethernet interface.

Syntax

show media interface { **ethernet** *slot/port* }

Parameters

ethernet *slot/port*

Specifies an Ethernet interface. The value for *slot* must be **0** for devices that do not support line cards.

Modes

Privileged EXEC mode

Examples

To display SPF information for an Ethernet interface:

```
device# show media interface ethernet 0/1
  Interface      Ethernet 0/1
  Identifier     3    SFP
  Connector      33   Copper Pigtail
  Transceiver           5500080000000000 10_GB/s
  Name           cu
  Encoding       0
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0    (units km)
  Length 9u      0    (units 100 meters)
  Length 50u     0    (units 10 meters)
  Length 62.5u   0    (units 10 meters)
  Length Cu      1    (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     00:05:1e
  Vendor PN      58-0000051-01    (4x10GE QSFP+ to 4 SFP+ copper cable - 1m)
  Vendor Rev     A
  Wavelength     N/A
  Options        0012
  BR Max         0
  BR Min         0
  Serial No      MAM2160400194JC1
  Date Code      160130
  Optical Monitor No
  Temperature    N/A
  Voltage        N/A
  Current        N/A
  TX Power       N/A
  RX Power       N/A
```

History

Release version	Command history
17s.1.00	This command was introduced.

show media optical-monitoring

Displays the configuration values and environmental information for optical interfaces.

Syntax

show media optical-monitoring

show media optical-monitoring interface [**ethernet** *slot/port*]

show media optical-monitoring supported-interfaces [**ethernet** *slot/port*]

Parameters

ethernet *slot/port*

Specifies an Ethernet interface. The value for *slot* must be **0** on devices that do not support line cards.

Modes

Privileged EXEC mode

Examples

The following displays sample output for all interfaces.

```
device# show media optical-monitoring
N/A - Not Available.
N/S - Optical Smart Data Not Supported.
Port        Optical    Module      Supply     Channel           Bias      Channel
            Monitoring Temperature Voltage    TX Power          Current   RX Power
            Support    ( C )       ( mVolts ) ( uWatts / dBm )  ( mAmps ) ( uWatts / dBm )
=========== ========== =========== ========== ================= ========= =================
Et 0/1      NO                                  N/S
Et 0/2      NO                                  N/S
Et 0/3      NO                                  N/S
Et 0/4      NO                                  N/S
Et 0/5      NO                                  N/S
Et 0/6      NO                                  N/S
Et 0/50     YES        34          3333.0     0.0 / -inf        7.138     882.8
/ -0.541
                                                                7.260     906.8
/ -0.425
                                                                7.046     862.9
/ -0.640
                                                                7.444     886.5
/ -0.523
```

The following displays sample output for a single Ethernet interface.

```
F115# show media optical-monitoring interface ethernet 0/1
N/A - Not Available.
N/S - Optical Smart Data Not Supported.
Port        Optical    Module      Supply     Channel           Bias      Channel
            Monitoring Temperature Voltage    TX Power          Current   RX Power
            Support    ( C )       ( mVolts ) ( uWatts / dBm )  ( mAmps ) ( uWatts / dBm )
=========== ========== =========== ========== ================= ========= =================
Et 0/1      NO                                  N/S
```

History

Release version	Command history
17s.1.00	This command was introduced.

show monitor

Displays the monitoring information for all Port Mirroring sessions or for a single session.

Syntax

show monitor [**session** *session_number*]

Parameters

session *session_number*

Specifies a session identification number. Valid values range from 0 through 511.

Modes

Privileged EXEC mode

Command Output

The **show monitor** command displays the following information:

Output field	Description
Session	The identifying value applied to the session
Type	The type of 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

To display monitoring information for all Port Mirroring sessions:

```
device# show monitor

Session                         :1
Type                            :Remote source session
Description                     :Test monitor session
State                           :Enabled
Source interface                :eth 0/1 (Up)
Destination interface           :Vlan x
Direction                       :Rx
```

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf

Displays the NETCONF session.

Syntax

show netconf

Modes

Privileged EXEC mode

Usage Guidelines

Because the text output is extensive, we recommend that you redirect 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>
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 that you redirect 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>
```

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf client-capabilities

Displays the client capabilities associated with each NETCONF session.

Syntax

show netconf client-capabilities

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display client capabilities for all active NETCONF sessions. It always displays the session-ID, login name of the user of the client session, the host IP address, and the time the user logged on. The application vendor name, application product name and version number, and the identity of the client are also returned if these values are advertized by the client as capabilities in the <hello> message to the server at the start of the session.

Command Output

The **show netconf client-capabilities** command displays the following information:

Output field	Description
Session Id	The numeral value assigned to identify the session.
User name	The user name of the account accessing NETCONF.
Vendor	The manufacturer of the device.
Product	The software product being utilized.
Version	The version number of the Product.
Client user	The client user name of the account accessing NETCONF.
Host IP	IP address for the current login.
Login time	Timestamp for the current login.

Examples

Typical command output example

```
device# show netconf client-capabilities

Session Id  : 10
User name   : root
Vendor      : Brocade
Product     : Brocade Network Advisor
Version     : 9.1.0 Build 123
Client user : admin-user
Host IP     : 10.24.65.8
Login time  : 2011-08-18T08:54:24Z
```

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf datastores

Displays the datastores available for NETCONF.

Syntax

show netconf datastores

Modes

Privileged EXEC mode

Examples

Typical output example for this command.

```
device# show netconf datastores
netconf-state datastores datastore running
 transaction-id 1488-921518-391273
netconf-state datastores datastore startup
```

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf files

Displays the files available on the NETCONF server

Syntax

show netconf files[*filename*]

Parameters

filename

The name of the NETCONF file to display.

Modes

Privileged EXEC mode

Examples

Typical command output example.

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf schemas

Displays the data models supported by the NETCONF server.

Syntax

show netconf schemas

Modes

Privileged EXEC mode

Examples

Typical output example for this command.

```
device# show netconf schemas
netconf-state schemas schema brocade-aaa 2010-10-21 yang
 namespace urn:brocade.com:mgmt:brocade-aaa
 location [ NETCONF ]
netconf-state schemas schema brocade-aaa-ext 2010-09-21 yang
 namespace urn:brocade.com:mgmt:brocade-aaa-ext
 location [ NETCONF ]
 location [ NETCONF ]
netconf-state schemas schema brocade-arp 2011-10-31 yang
 namespace urn:brocade.com:mgmt:brocade-arp
 location [ NETCONF ]
netconf-state schemas schema brocade-bfd 2014-09-24 yang
 namespace urn:brocade.com:mgmt:brocade-bfd
 location [ NETCONF ]
netconf-state schemas schema brocade-bgp 2010-11-29 yang
 namespace urn:brocade.com:mgmt:brocade-bgp
 location [ NETCONF ]
netconf-state schemas schema brocade-bridge-domain 2011-06-21 yang
 namespace urn:brocade.com:mgmt:brocade-bridge-domain
 location [ NETCONF ]
netconf-state schemas schema brocade-certutil 2011-06-13 yang
 namespace urn:brocade.com:mgmt:certutil
 location [ NETCONF ]
netconf-state schemas schema brocade-chassis 2011-04-11 yang
 namespace urn:brocade.com:mgmt:brocade-chassis
 location [ NETCONF ]
<output truncated>
```

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf sessions

Displays the currently active NETCONF sessions .

Syntax

show netconf sessions

Modes

Privileged EXEC mode

Examples

Typical output example for this command.

```
device# show netconf sessions
netconf-state sessions session 9
 transport cli-console
 username admin
 source-host 127.0.0.1
 login-time 2017-03-04T19:58:55+00:00
netconf-state sessions session 34
 transport cli-console
 username admin
 source-host 10.252.138.8
 login-time 2017-03-07T21:59:52+00:00
```

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf statistics

Displays statistics related to the NETCONF server.

Syntax

show netconf statistics

Modes

Privileged EXEC nmode

Examples

Typical output example for this command.

```
device# show netconf statistics
netconf-state statistics netconf-start-time 2017-03-04T19:09:16+00:00
netconf-state statistics in-bad-hellos 0
netconf-state statistics in-sessions 0
netconf-state statistics dropped-sessions 0
netconf-state statistics in-rpcs 0
netconf-state statistics in-bad-rpcs 0
netconf-state statistics out-rpc-errors 0
netconf-state statistics out-notifications 0
```

History

Release version	Command history
17s.1.00	This command was introduced.

show netconf-state datastores

Displays the NETCONF datastores that are present on the NETCONF server along with related locking information.

Syntax

show netconf-state datastores

Modes

Privileged EXEC mode

Command Output

The **show netconf-state datastores** command displays the following information:

Output field	Description
Name	Designates either the running or startup datastore.
Locked by Session	Displays if the datastore is locked.
Locked Time	Displays when the datastore was locked.
Lock ID	Displays the lock identification.
Locked by Session	Displays the session
Locked Time	Displays the duration of the datastore lock.
Select	Displays the selection status of the datastore.
Locked Node	Displays the node information of the datastore lock.

Examples

Typical command output example.

```
device# show netconf-state datastores

         LOCKED                  LOCKED
         BY       LOCKED  LOCK   BY       LOCKED          LOCKED
NAME     SESSION  TIME    ID     SESSION  TIME    SELECT  NODE
-----------------------------------------------------------------
running  -        -
startup  -        -
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ntp status

Displays the Network Time Protocol (NTP) status.

Syntax

show ntp status

Modes

User EXEC mode

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 an NTP server is not configured:

```
device# show ntp status

active ntp server is LOCL
```

To show the configured NTP server:

```
device# show ntp status

active ntp server is 10.21.2.80
```

History

Release version	Command history
17s.1.00	This command was introduced.

show overlay-class-map

Displays configurations for all overlay class maps or a specified map.

Syntax

show overlay-class-map [*name*]

Parameters

name

Displays configurations for the specified overlay class map.

Modes

Privileged EXEC mode

Examples

To display configurations for a specified overlay class map:

```
device# show overlay-class-map OVER_CLASS_1
overlay-class-map
  Configuration:
    seq 1 match source 10.1.0.1 destination 20.1.0.1 encap-type vxlan
    seq 2 match source 10.1.0.2 destination 20.1.0.2 encap-type vxlan
    seq 3 match source 10.1.0.3 destination 20.1.0.3 encap-type vxlan
    seq 4 match source 10.1.0.4 destination 20.1.0.4 encap-type vxlan
  Referenced Overlay-Policy-Maps:
      BASIC_KEYTYPE_VERIFY seq 10
```

History

Release version	Command history
17s.1.01	This command was introduced.

show overlay-policy-map

Displays configurations for all overlay policy maps or a specified map.

Syntax

show overlay-policy-map [*name*]

Parameters

name

Displays details for the specified overlay policy map.

Modes

Privileged EXEC mode

Examples

To display configurations for a specified overlay policy map:

```
device# show overlay-policy-map BASIC_KEYTYPE_VERIFY
overlay-policy-map BASIC_KEYTYPE_VERIFY
  Configuration:
    seq 10 overlay-class OVER_CLASS_1
      ip access-group IPv4ACL_High_KT0
    seq 20 overlay-class OVER_CLASS_2
      ip access-group IPv4ACL_High_KT1
    seq 30 overlay-class OVER_CLASS_3
      ip access-group IPv4ACL_High_KT2
    seq 40 overlay-class OVER_CLASS_4
      ip access-group IPv4ACL_High_KT3
  Active On:
    Overlay-transit BASIC_VERIFICATION
```

History

Release version	Command history
17s.1.01	This command was introduced.

show overlay-service-policy

Displays currently active overlay service policy maps and they interfaces on which they are applied.

Syntax

show overlay-service-policy [*name*] [**detail**]

Parameters

name

Displays details for the specified overlay policy map.

detail

Displays details, including interfaces, on which one or all service policy maps are applied.

Modes

Privileged EXEC mode

Examples

To display all overlay service policy maps:

```
Device# show overlay-service-policy
Overlay-transit BASIC_VERIFICATION
    Ingress policy BASIC_KEYTYPE_VERIFY
```

To display the details of a specified overlay service policy map:

```
device# show overlay-service-policy BASIC_KEYTYPE_VERIFY
overlay-policy-map BASIC_KEYTYPE_VERIFY
  Overlay-transit BASIC_VERIFICATION at Ingress
    seq 10 overlay-class OVER_CLASS_1 (Active)
      ip access-group IPv4ACL_High_KT0 (Active)
    seq 20 overlay-class OVER_CLASS_2 (Active)
      ip access-group IPv4ACL_High_KT1 (Active)
    seq 30 overlay-class OVER_CLASS_3 (Active)
      ip access-group IPv4ACL_High_KT2 (Active)
    seq 40 overlay-class OVER_CLASS_4 (Active)
      ip access-group IPv4ACL_High_KT3 (Active)
```

To display details, including interfaces, for a specified overlay service policy map:

```
device# show overlay-service-policy BASIC_KEYTYPE_VERIFY detail
overlay-policy-map BASIC_KEYTYPE_VERIFY
  Overlay-transit BASIC_VERIFICATION at Ingress
    seq 10 overlay-class OVER_CLASS_1 (Active)
        seq 1 match source 10.1.0.1 destination 20.1.0.1 encap-type vxlan (Active)
        seq 2 match source 10.1.0.2 destination 20.1.0.2 encap-type vxlan (Active)
        seq 3 match source 10.1.0.3 destination 20.1.0.3 encap-type vxlan (Active)
        seq 4 match source 10.1.0.4 destination 20.1.0.4 encap-type vxlan (Active)
      ip access-group IPv4ACL_High_KT0 (Active)
    seq 20 overlay-class OVER_CLASS_2 (Active)
        seq 1 match source 10.2.0.1 destination 20.2.0.1 encap-type vxlan (Active)
        seq 2 match source 10.2.0.2 destination 20.2.0.2 encap-type vxlan (Active)
        seq 3 match source 10.2.0.3 destination 20.2.0.3 encap-type vxlan (Active)
        seq 4 match source 10.2.0.4 destination 20.2.0.4 encap-type vxlan (Active)
      ip access-group IPv4ACL_High_KT1 (Active)
    seq 30 overlay-class OVER_CLASS_3 (Active)
        seq 1 match source 10.3.0.1 destination 20.3.0.1 encap-type vxlan (Active)
        seq 2 match source 10.3.0.2 destination 20.3.0.2 encap-type vxlan (Active)
        seq 3 match source 10.3.0.3 destination 20.3.0.3 encap-type vxlan (Active)
        seq 4 match source 10.3.0.4 destination 20.3.0.4 encap-type vxlan (Active)
      ip access-group IPv4ACL_High_KT2 (Active)
    seq 40 overlay-class OVER_CLASS_4 (Active)
        seq 1 match source 10.4.0.1 destination 20.4.0.1 encap-type vxlan (Active)
        seq 2 match source 10.4.0.2 destination 20.4.0.2 encap-type vxlan (Active)
        seq 3 match source 10.4.0.3 destination 20.4.0.3 encap-type vxlan (Active)
        seq 4 match source 10.4.0.4 destination 20.4.0.4 encap-type vxlan (Active)
      ip access-group IPv4ACL_High_KT3 (Active)
```

History

Release version	Command history
17s.1.01	This command was introduced.

show packet-encap-processing

Displays information about the interfaces on which header processing is enabled.

Syntax

show packet-encap-processing

Modes

Privileged EXEC mode

Usage Guidelines

Ths command is relevant only in NPB system mode.

Command Output

The **show packet-encap-processing** command displays the following information:

Output field	Description
Port	Displays the Ethernet slot and port.
Link	Displays "Up" or "Down".
Encapsulation	Displays the header-stripping type.
Status	If the header-stripping option is enabled on an interface, but not yet programmed in hardware—by a linecard or system reload—displays "Inactive". If the header-stripping option is enabled on an interface and is also programmed in hardware, displays "Active".

Examples

The following example displays a typical run of **show packet-encap-processing**.

```
show packet-encap-processing

Total number of packet-encap-processing interfaces: 6

------------------------------------------------------------
Port       Link     Encapsulation        Status
------------------------------------------------------------
eth 0/1    Down     802.1BR Stripping    Active
eth 0/2    Down     802.1BR Stripping    Active
eth 0/3    Down     VN-Tag Stripping     Active
eth 0/4    Up       VN-Tag Stripping     Active
eth 0/5    Up       VXLAN Stripping      Inactive
eth 0/6    Up       VXLAN Stripping      Inactive
```

History

Release version	Command history
18s.1.00	This command was introduced.

show pbf destination

Displays information about one PBF destination or about all PBF destinations.

Syntax

show pbf destination [*destination-id*]

Parameters

destination-id

Specifies a PBF destination.

Modes

Privileged EXEC mode

Usage Guidelines

The use-case for this command is under Network Packet Broker (NPB) system mode.

Command Output

The **show pbf destination** command displays the following information:

Output field	Description
Destination Id	Displays the destination ID.
Interface Name	Displays the physical and port-channel interfaces defined for the destination.

Examples

The following example is typical output of the basic form of this command.

```
device# show pbf destination
Destination Id    Interface Name
==============    ==============
1000              ethernet 0/1 type-fabric
                  ethernet 0/2 type-fabric (selected)
                  Counts: packets:0 bytes:0

2000              port-channel 8 (selected)
                  ethernet 0/2
                  Counts: packets:0 bytes:0

3000              ethernet 0/2 (selected)
                  ethernet 0/21
                  Counts: packets:0 bytes:0
```

History

Release version	Command history
18s.1.02	This command was introduced.

show pbf destination-group

Displays information about one PBF destination-group or about all PBF destination-groups.

Syntax

show pbf destination-group [*pbf-group-id*]

Parameters

pbf-group-id

Specifies a policy-based forwarding (PBF)-destination group. Values range from 1 through 8192.

Modes

Global configuration mode

Usage Guidelines

The use-case for this command is under Network Packet Broker (NPB) system mode.

Command Output

The **show pbf destination-group** command displays the following information:

Output field	Description
Destination-Group ID	Displays the destination-group ID.
Members	Displays the destination ID.
Interface Name	Displays the physical and port-channel interfaces defined for the destination.

Examples

The following example is typical output of the basic form of this command.

```
device# show pbf destination-group
Destination-Group ID   Members    Interface Name
====================   =======    ==============
10                     1000       ethernet 0/1 type—fabric
                                  ethernet 0/2 type-fabric (selected)
                                  Counts: packets:0 bytes:0

                       2000       port—channel 8 (selected)
                                  ethernet 0/2
                                  Counts: packets:0 bytes:0

20                     3000       ethernet 0/2 (selected)
                                  ethernet 0/21
                                  Counts: packets:0 bytes:0
```

History

Release version	Command history
18s.1.02	This command was introduced.

show policy-map

Displays configured policy-maps and class-map Policer parameters applied to switch interfaces.

Syntax

show policy-map [**detail** *policyname* | **interface** { **ethernet** *0/port* | **port-channel** *number* } [**in** | **out**]]

Parameters

details *policyname*
Displays the detail configuration of the policy-map along with binding information.

ethernet *0/port*
Specifies the Ethernet interface port number.

port-channel *number*
Specifies the port channel number.

in
Inbound direction where the policy map is applied.

out
Outbound direction where the policy map is applied.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

Use this command with a specific interface to display the policy map binding settings (policy map name and traffic direction), police-priority-map applied, and class map policer parameters applied for that interface.

Use this command without identifying an interface and direction of traffic to display policy map binding for all interfaces on the switch.

Command 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.

Output field	Description
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.
set-dscp	The DSCP value which is applied to the traffic for the given color (conform, exceed, violate).
set-tc	The remapped traffic class queue for the traffic for the given color (conform, exceed, violate).
Total	The total traffic in bytes carried on this interface for the defined rate-limit policy.

Examples

To display policy-map binding and class map parameters applied to a specific interface:

```
device# show policy-map interface ethernet 0/1 in
Interface : Ethernet 0/1
policy-map: policy-mapA-1
Direction: Input
Input Excluded lossless priorities: None

Class-map: default
    Police:
        cir 5 bps cbs 5678 bytes eir 512000 bps ebs 4096 bytes
        Police-priority-map: po-pr-map1
        Conformed: 30720 bytes set-dscp 0 set-tc 0
        Exceeded: 23424 bytes set-dscp 0 set-tc 0
        Violated: 0 bytes
        Total: 54144 bytes
```

To display policy map binding information for all interfaces:

```
device# show policy-map
Interface : Ethernet 0/2
Inbound policy map is policy-mapA-1
Outbound policy map is not set
Interface : Ethernet 0/3
Inbound policy map is not set
Outbound policy map is not set
Interface : Ethernet 0/4
Inbound policy map is not set
Outbound policy map is not set
```

History

Release version	Command history
17s.1.00	This command was introduced.

show port port-channel ethernet

Displays the detailed LACP attributes that are configured and negotiated with its partner.

Syntax

show port port-channel ethernet *slot* **/** *port*

Parameters

slot

Specifies a valid slot. Must be `0`.

port

Specifies a valid port.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show port-channel

Displays the Link Aggregation Group (LAG) information for a port-channel.

Syntax

show port-channel [*channel-group-number* | **detail** | **load-balance** | **summary**]

Parameters

channel-group-number
Specifies a port-channel number to display. Range is from 1 through 1024.

detail
Displays detailed LAG information for a port-channel.

load-balance
Displays the load-balance or frame-distribution scheme among ports in the 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** 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
 Static Aggregator: Po 1
 Aggregator type: Standard
```

The following example displays summary output.

```
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show port-channel detail

The **show port-channel detail** command displays the Link Aggregation Group (LAG) information for a port-channel.

Syntax

show interface port channel [*channel-group-number*|**detail**|**load-balance**|**summary**]

Parameters

channel-group-number
Specifies a LAG port channel-group number to display. The number of available channels range from 1 through 6144.

detail
Displays detailed LAG information for a port-channel.

load-balance
Displays detailed LAG information for a port-channel.

summary
Displays the summary information per channel-group.

Modes

Privileged EXEC

Usage Guidelines

Use this command to display the LAGs present on the system.

Examples

This example shows how to display detail information for a specific port channel:

```
SLX# show port-channel detail
 Static Aggregator: Po 20
 Aggregator type: Standard
 Insight mode is enabled
 Number of Ports: 1
SLX#
```

History

Release version	Command history
17s.1.01	This command was introduced.

show port-channel summary

To display summary information about the port channels, use the **show port-channel summary** command.

Syntax

show port-channel summary

Modes

EXEC

Command Output

The **show port-channel summary** command displays the following information:

Output field	Description
`D - Down`	Interface is Up in port-channel members.
`U - Up (Port-channel)`	Primary link in port-channel.
`S- Switched`	Insight Enabled.
`M - Not in use. Min-links not met`	

Examples

This example shows how to display summary information for the port channels:

```
SLX# show port-channel summary
Flags:  D - Down               P - Up in port-channel (members)
        U - Up (port-channel)  * - Primary link in port-channel
        S - Switched           I - Insight Enabled
        M - Not in use. Min-links not met
===== =============== ========== ===============
Group Port-channel    Protocol   Member ports
===== =============== ========== ===============
20    Po 20   (UI)    None
SLX#
```

History

Release version	Command history
17s.1.01	This command was introduced.

show port-security

Displays the configuration information related to port security.

Syntax

show port-security [**addresses** | **interface ethernet** *slot/port*]

Parameters

addresses

Displays the secure MAC addresses configured on the device.

interface

Specifies an interface.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port. The slot number must be 0 if the switch does not contain slots.

Modes

Privileged EXEC mode

Interface configuration mode

Command 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. Action will be either Restrict or Shutdown.
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. Violation Mode will be verified for Restrict and Shutdown configuration.
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.

Output field	Description
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-0/2)# do show port-security
Secure    MaxSecureAddr  CurrentAddr  StaticSec  Violated  Action    Sticky
Port         (count)       (count)     (count)
Eth 0/2       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-0/2)# do show port-security interface ethernet 0/2
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-0/2)# do show port-security addresses
                    Secure Mac Address Table
------------------------------------------------------------------
Vlan       Mac-address            Type                    Ports
250        3200.1110.0002         Secure-Static           Eth 0/2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 switch.

For an explanation of process states, refer to the UNIX manual page for the **ps** command.

Examples

To show the information for 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
```

To show CPU usage information by individual 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)
```

To show the information for all partitions:

```
device# show process cpu all-partitions
Load Average:
L1/0:    2.81    2.27    2.15
L1/1:    2.00    2.00    2.00
L2/0:    2.00    2.01    2.00
L2/1:    2.06    2.03    2.00

Total CPU Utilization (in %):
L1/0:    4.39    0.14    3.83    0.41
L1/1:    0.5    0.00    0.08    0.42
L2/0:    0.49    0.01    0.05    0.44
L2/1:    0.5    0.01    0.05    0.44
```

History

Release version	Command history
17s.1.00	This command was introduced.

show process info

Displays system processes hierarchically.

Syntax

show process info]

Command Default

This command is executed on the local switch.

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

To display system processes hierarchically:

```
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]
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 switch.

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]
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ptp brief

Displays the status of each physical port that has a running Precision Time Protocol (PTP) session, and for port channels the status of each member port that has a running PTP session.

Syntax

show ptp brief

Modes

Privileged EXEC mode

Command Output

The **show ptp brief** command displays the following information if the state is Disabled:

Disabled reason code	Description
Link Down	Physical link state is Down
STP Block	Port is blocked by STP
None	PTP is globally disabled

Examples

The following displays example output:

```
device# show ptp brief
Port            PTP Port State
-------  --------------
Eth 0/1      Disabled(Link Down)
Eth 0/2      Passive
Eth 0/3      Master
Eth 0/4      Slave
Eth 0/5      Disabled(STP Block)
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ptp clock

Displays the status of a local Precision Time Protocol (PTP) clock.

Syntax

show ptp clock

Modes

Privileged EXEC mode

Examples

The following displays example output:

```
device# show ptp clock
Clock Type: Boundary clock
Clock Identity: 60:9c:9f:ff:fe:87:3b:00
Clock Domain: 0
Clock State: Time Synced
Number of PTP ports: 5
Priority1 : 255
Priority2 : 255
Clock Quality:
        Class : 248
        Accuracy : 254
        Offset (log variance) : 65535
Offset From Master: -0.000000360
Mean Path Delay: +0.000000070
Steps removed: 1
Local clock time: Thu Apr 30 06:26:59 2015
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ptp clock foreign-masters record

Displays the status of foreign master clocks known to a Precision Time Protocol (PTP) clock. For each foreign master clock, the output displays the clock identity, basic clock properties, and whether the clock is being used as a grandmaster clock.

Syntax

show ptp clock foreign-masters record

Modes

Privileged EXEC mode

Examples

The following displays example output:

```
device# show ptp clock foreign-masters record
P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed

---------   ----------------------  ---  ----  ----  ---  -----  --------
Interface         Clock-ID          P1   P2    C     A    OSLV   SR
---------   ----------------------  ---  ----  ----  ---  -----  --------
Eth 0/1      60:9c:9f:ff:fe:87:3b:00 128   128   248   254  65535  1
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ptp corrections

Displays the recent history of Precision Time Protocol (PTP) local clock offset adjustments.

Syntax

show ptp corrections

Modes

Privileged EXEC mode

Examples

The following displays example output:

```
device# show ptp corrections
PTP past corrections
------------------------------------------------------------
Slave Port          SUP Time                  Correction(ns)
----------  ----------------------------  ------------------
Eth 0/1       Thu Apr 16 01:20:17 2015       354
Eth 0/1       Thu Apr 16 01:20:18 2015      -760
Eth 0/1       Thu Apr 16 01:20:19 2015      -315
Eth 0/1       Thu Apr 16 01:20:20 2015       -83
Eth 0/1       Thu Apr 16 01:21:53 2015       260
Eth 0/1       Thu Apr 16 01:21:54 2015       117
…
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ptp parent

Displays properties of the Precision Time Protocol (PTP) parent clock port.

Syntax

show ptp parent

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following displays example output:

```
device# show ptp parent
Parent Clock:
Parent Clock Identity: 60:9c:9f:ff:fe:87:3b:00
Parent Port Number: 5
Parent IP Address: 0.0.0.0
Observed Parent Offset (log variance): 65535
Observed Parent Clock Phase Change Rate: 2147483647

Grandmaster Clock:
Grandmaster Clock Identity: 60:9c:9f:ff:fe:87:3b:00
Grandmaster Clock Quality:
   Class: 248
   Accuracy: 254
   OffsetScaledLogVariance: 65535
   Priority1: 100
   Priority2: 255
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ptp port interface

Displays the properties and statistics of a Precision Time Protocol (PTP) interface.

Syntax

show ptp port interface [*interface*]

Parameters

interface

Name of a PTP-enable interface.

Modes

Privileged EXEC mode

Usage Guidelines

For a port-channel interface, there is a maximum of two member interfaces for each remote node that is a member of the Multi-Chassis Trunk (MCT).

A port type of "local" indicates that the PTP session is initiated locally. For a physical interface, the PTP port type is always set to "local".

A port type of "remote" indicates that the PTP session is remotely initiated.

Examples

The following is example output for a port-channel interface:

```
device# show ptp port interface port-channel 10
PTP Port Dataset: Eth 0/1
Port identity: clock identity:  60:9c:9f:ff:fe:87:3b:00
Port identity: port number: 5
PTP version: 2
Port state: Master
Port Type: local
VLAN info:  1
Delay request interval (log mean): 1
Announce receipt time out: 3
Peer mean path delay: 0
Announce interval (log mean): 1
Sync interval (log mean): 1
Delay Mechanism: End to End
Transport mode: ipv4
Announce messages sent: 15
Announce messages received: 2
Sync messages sent: 30
Sync messages received: 0
Follow up messages sent: 30
Follow up messages received: 0
Delay request messages sent: 0
Delay request messages received: 30
Delay response messages sent: 30
Delay response messages received: 0


PTP Port Dataset: Eth 0/1
Port identity: clock identity:  60:9c:9f:ff:fe:87:3b:00
Port identity: port number: 6
PTP version: 2
Port state: Master
Port Type: remote
VLAN info:  1
Delay request interval (log mean): 1
Announce receipt time out: 3
Peer mean path delay: 0
Transport mode: ipv4
Announce messages sent: 15
Announce messages received: 0
Sync messages sent: 30
Sync messages received: 0
Follow up messages sent: 30
Follow up messages received: 0
Delay request messages sent: 0
Delay request messages received: 30
Delay response messages sent: 30
Delay response messages received: 0
```

The following is example output for an Ethernet interface:

```
sw0# show ptp port interface ethernet 0/2
PTP Port Dataset: Eth 0/2
Port identity: clock identity:  60:9c:9f:ff:fe:87:3b:00
Port identity: port number: 10
PTP version: 2
Port state: Master
Port Type: local
VLAN info:  1
Delay request interval (log mean): 1
Announce receipt time out: 3
Peer mean path delay: 0
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ptp time-property

Displays the properties of the Precision Time Protocol (PTP) clock.

Syntax

show ptp time-property

Modes

Privileged EXEC mode

Examples

The following is example output:

```
device# show ptp time-property
PTP CLOCK TIME PROPERTY:
        Current UTC Offset valid: 1
        Current UTC Offset: 35
        Leap59: 0
        Leap61: 0
        Time Traceable: 0
        Frequency Traceable: 0
        PTP Timescale: 1
        Time Source:  160 (Internal Source)
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos cpu queue

Displays the protocol-to-CPU queue mapping or FPS for the specified central processing unit (CPU) queue.

Syntax

show qos cpu queue { **info** | *queue-number* }

Parameters

info

Displays the protocol-to-CPU queue mapping. The information includes the frames per second (FPS) rate and priority.

queue-number

Specifies the CPU queue number to display its default and current FPS. Enter an integer from 0 through 31. You can display an individual queue or a range of queues. To display a range of queues, insert a hyphen between the beginning and ending integers (for example, 5-16). To display individual queues and ranges of queues, separate them by commas (for example, 1,2,4-7,8,9-22,55-66). You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Command Output

The **show qos cpu queue info** command displays the following information:

Output field	Description
CPU Queue	Number of the CPU queue.
FPS	Packet rate for the queue in frames per second.
Priority	Priority of the queue.
Usage	Protocol mapped to the queue .
Unused Credits	Remaining packets that are available for configuration to a queue.

The **show qos cpu queue** *queue-number* command displays the following information:

Output field	Description
Queue	Number of the CPU queue.
Default FPS	Default packet rate for the queue in frames per second.
Current FPS	Configured packet rate for the queue in frames per second.
Unused Credits	Remaining packets that are available for configuration to a queue.

Examples

The following example displays all CPU queues on the device, including their associated protocols, current frame rates, priorities, and unused credits.

```
device# show qos cpu queue info
================================================================================
CPU
Queue  FPS    Priority  Usage
================================================================================
0      1000   0         Sflow
1       256   1         ACL Log
2       256   2         LPM Hit,LPM Miss
3      4096   0         Unused
4      8192   4         SA MAC Learning,DA MAC Learning
5       384   0         Unused
6        64   6         DAI
7       300   7         MyIP
8       384   8         ARP Suppression Request,ARP Request,VRRP ARP Request,
                        ND Suppression Request,ND Request
9       128   9         Router Solicitations
10      512   10        IGMP
11      256   11        PIM
12      256   12        MLD
13     1500   13        DHCP Request
14      512   14        MyIP Telnet,MyIP SSH
15        0   0         Unused
16     1500   16        OSPF
17     1500   17        BGP
18      768   18        ARP Response,ND Response
19     1500   19        DHCP Response
20     2048   20        VRRP,VRRPE
21       32   21        MyIP Ping
22      128   0         Unused
23      256   23        802.1X
24      128   24        LLDP
25      512   25        PTP
26     1024   26        CTP
27     2048   27        BFD
28      256   0         Unused
29      128   0         Unused
30     2176   30        STP,PVST
31      128   31        LACP
================================================================================
Unused Credits: 20
================================================================================
```

The following example displays the specified CPU queues with their default and current FPS rates, and unused credits.

```
device# show qos cpu queue 0-3
Queue 0
  Default FPS: 1000
  Current FPS: 1400
Queue 1
  Default FPS: 256
  Current FPS: 300
Queue 2
  Default FPS: 1000
  Current FPS: 300
Queue 3
  Default FPS: 4000
  Current FPS: 0
Unused Credits: 1000
```

History

Release version	Command history
17s.1.01	This command was introduced.

show qos flowcontrol interface

Displays all of the configured flow control information for an interface.

Syntax

show qos flowcontrol interface [**ethernet 0/***port* | **all** | **port-channel** *number*]

Parameters

ethernet 0/*port*

Specifies the Ethernet interface. Enter a valid port number.

all

Reports QoS flow control statistics for all interfaces within the system.

port-channel *number*

Specifies the port channel.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the runtime state retrieved frm the dataplane reflecting the operation of 802.3x pause or Priority Flow Control (PFC) on an interface.

The administrative state for pause generation and reception or processing is presented for the interface (802.3x mode) or for each CoS (PFC mode). TX_Pause frame generation statistics are always presented for the interface. The RX_Pause BitTimes is presented for the interface (802.3x mode) or for each CoS (PFC mode). When PFC is deployed under the CEE Provisioning model, then the command reports whether the Data Center Bridging eXchange protocol (DCBX) has overridden the user configuration, for example when the DCBX detects a mis-configuration between CEE peers, it disables PFC operationally.

Examples

To display all of the configured flow control information for an Ethernet interface:

```
device# show qos flowcontrol interface ethernet 0/1

Interface ethernet 0/1
  Mode PFC
  DCBX enabled for PFC negotiation
  TX 0 frames
         TX   TX    RX   RX Output Paused
  CoS Admin Oper Admin Oper  512 BitTimes
  ---------------------------------------
    0   Off  Off   Off  Off             0
    1   Off  Off   Off  Off             0
    2    On  Off    On  Off             0
    3   Off  Off   Off  Off             0
    4   Off  Off   Off  Off             0
    5   Off  Off   Off  Off             0
    6   Off  Off   Off  Off             0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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 Ethernet 0/1:1
  Provisioning Mode: none
  Default CoS: 0
  Default TC: 1
  Interface CoS Trust: untrusted
  Interface DSCP Trust: untrusted

  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 0/2:1
  Provisioning Mode: none
  Default CoS: 0
  Default TC: 1
  Interface CoS Trust: untrusted
  Interface DSCP Trust: untrusted

  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 0/3:1
  Provisioning Mode: none
  Default CoS: 0
  Default TC: 1
  Interface CoS Trust: untrusted
  Interface DSCP Trust: untrusted

  Flow control mode Off
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos interface ethernet

Displays QoS configuration information for a specific Ethernet interface.

Syntax

show qos interface ethernet 0/*port*

Parameters

port

Specifies a port number.

Modes

Privileged EXEC mode

Examples

The example displays the QoS configuration for a specific interface.

```
device# show qos interface ethernet 0/9
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 0/9
  Provisioning Mode: none
  Default CoS: 0
  Default TC: 1
  Interface CoS Trust: untrusted
  Interface DSCP Trust: untrusted

  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


  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

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Examples

The following example displays 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 Port-channel 20
  Provisioning Mode: none
  Default CoS: 0
  Default TC: 1
  Interface CoS Trust: untrusted
  Interface DSCP Trust: untrusted

  Flow control mode Off

  Traffic Class Scheduler configured for 1 Strict Priority queues
      TrafficClass:   0   1   2   3   4   5   6   7
      ------------------------------------------------
        DWRRWeight:   0   0  25  15  10  15  20 ---
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos maps cos-traffic-class

Displays the configured QoS CoS-to-traffic class mutation maps.

Syntax

show qos maps cos-traffic-class [*map-name*]

Parameters

map-name

Specifies the name of the CoS-to-traffic class map.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a map name, this command displays all CoS-to-traffic class maps.

Examples

The following example displays a CoS-to-traffic class map.

```
device# show qos maps cos-traffic-class cosTCMap
  [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

 Cos-to-TC map: cosTCMap
             In-CoS: 0  1  2  3  4  5  6  7
      ----------------------------------
             Out-TC: 0  1  2  3  3  6  6  6
             Out-DP: 0  0  0  0  0  0  0  0

       Enabled on the following interfaces:
    Eth 0/4
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos maps dscp-cos

Displays configured DSCP-to-CoS mutation maps.

Syntax

show qos maps dscp-cos [*map-name*]

Parameters

map-name

Specifies the name of the DSCP-to-CoS mutation map.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a map name, this command displays all DSCP-to-CoS mutation maps.

Examples

The following example displays a DSCP-to-CoS map applied to an interface.

```
device#  show qos maps dscp-cos dscpCosMap
 [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]


DSCP-to-CoS Map:  dscpCosMap (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 0/3
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos maps dscp-mutation

Displays configured DSCP mutation maps.

Syntax

show qos maps dscp-mutation [*map-name*]

Parameters

map-name

Specifies the name of the DSCP mutation map.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a map name, this command displays all DSCP mutation maps.

Examples

The following example displays a DSCP mutation map and its applied interface.

```
device# show qos map dscp-mutation dscpMap
  [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

  DSCP Mutation Map: dscpMap (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ----------------------------------------
       0 :    00 00 00 00 00 00 00 00 00 00
       1 :    00 00 00 00 00 00 00 00 00 00
       2 :    00 00 00 00 50 00 00 00 00 00
       3 :    00 00 00 35 00 00 00 00 00 00
       4 :    00 00 00 00 00 00 00 00 00 00
       5 :    00 00 00 61 00 00 00 00 00 00
       6 :    40 00 00 00

      Enabled on the following interfaces:
    Eth 0/3
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos maps dscp-traffic-class

Displays configured DSCP-to-traffic class mutation maps.

Syntax

show qos maps dscp-traffic-class [*map-name*]

Parameters

map-name

Specifies the name of the DSCP-to-traffic class map.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a map name, this command displays all DSCP-to-traffic class maps.

Examples

The following example displays a DSCP-to-traffic class mutation map.

```
device# show qos maps dscp-traffic-class dscpTcMap
 [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

  DSCP-to-TC Map: dscpTcMap (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 :     3/0 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 :     4/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 3/0 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 0/4
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos maps traffic-class-cos

Displays configured traffic class to CoS mutation maps.

Syntax

show qos maps traffic-class-cos [*map-name*]

Parameters

map-name

Specifies the name of a traffic class to CoS mutation map.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a map name, this command displays all traffic class to CoS mutation maps.

Examples

The following example displays a traffic class to CoS mutation map.

```
device# show qos maps traffic-class-cos tc1
  [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

  TC-to-CoS Map: test1
              In-TC: 0  1  2  3  4  5  6  7
      ------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  6  6  7
      Out-CoS(DP=1): 0  1  2  3  4  6  6  7
      Out-CoS(DP=2): 0  1  2  3  4  6  6  7
      Out-CoS(DP=3): 0  1  2  3  4  6  6  7
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos maps traffic-class-dscp

Displays configured traffic class to DSCP mutation maps.

Syntax

show qos maps traffic-class-dscp [*map-name*]

Parameters

map-name

Specifies the name of a traffic class to DSCP mutation map.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a map name, this command displays all traffic class to DSCP mutation maps.

Examples

The following example displays a traffic class to DSCP mutation map.

```
device# show qos maps traffic-class-dscp tcdscp1
  [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

  TC-to-DSCP Map: tcdscp1
              In-TC:  0   1   2   3   4   5   6   7
      ----------------------------------------------
           Out-DSCP: 00  08  16  24  55  40  48  56
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos maps traffic-class-mutation

Displays configured traffic class mutation maps.

Syntax

show qos maps traffic-class-mutation [*map-name*]

Parameters

map-name

Specifies the name of a traffic class mutation map.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a map name, this command displays all traffic class mutation maps.

Examples

The following example displays a traffic class mutation map.

```
device# show qos maps traffic-class-mutation tcm1
   [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

  TC Mutation Map: tcm1
              In-TC: 0  1  2  3  4  5  6  7
      ------------------------------------
             Out-TC: 0  1  2  3  0  5  6  7
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos red profiles

Displays configured Random Early Detect (RED) profiles.

Syntax

show qos red profiles

Modes

Privileged EXEC mode

Examples

The following example displays the applied RED profiles for a specific interface:

```
device# show qos red profiles
Red Profile 200
    Minimum Threshold: 40
    Maximum Threshold: 60
    Drop Probability: 40

Applied on the following interfaces:
Eth 0/1 Traffic-class: 4
```

History

Release version	Command history
17s.1.00	This command was introduced.

show qos red statistics

Displays the WRED statistics for an interface.

Syntax

show qos red statistics interface *interface-name*

Parameters

interface *interface-name*
Specifies the interface.

Modes

Privileged EXEC

Examples

The following example displays the WRED statistics for an interface.

```
device# show qos red statistics interface Eth 0/1
Statistics for interface: Eth 0/1
     Traffic-class: 2, ProfileId: 20
     Packets Dropped: Red: 0, Yellow: 0, Green: 0, Queue Drops: 0
     Bytes Dropped: Red: 0, Yellow: 0, Green: 0, Queue Drops: 0

Traffic-class: 3, ProfileId: 10
     Packets Dropped: Red: 0, Yellow: 0, Green: 0, Queue Drops: 0
     Bytes Dropped: Red: 0, Yellow: 0, Green: 0, Queue Drops: 0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

To display the runtime egress queue state information retrieved from the dataplane:

```
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show route-map

Displays the route map configuration details.

Syntax

show route-map [*name*]

show route-map [**interface** { **ethernet** *slot* **/** *port* | **ve** *ve-number*]

Parameters

name

Specifies a route-map.

interface ethernet *slot* **/** *port*

Specifies a physical interface. If the device has no slots, the slot value must be 0.

ve *ve-number*

Specifies a Virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Examples

The following command displays general route-map information.

```
device# show route-map
Interface Ethernet 0/6
 ip policy route-map route1
```

The following command displays the configured routing attributes of a specific route map.

```
device# show route-map route1
Interface Ethernet 0/6
ip policy route-map route1 permit 1 (Active)
    match ip address acl test1
    set ip next-hop 6.0.0.1 (selected)
    Policy routing matches: 1443 packets
```

The following command displays route-map configuration details for a specific interface.

```
device# show route-map interface ethernet 0/6
Interface Ethernet 0/6
ip policy route-map route1 permit 1 (Active)
    match ip address acl test1
    set ip next-hop 6.0.0.1 (selected)
    Policy routing matches: 1543 packets
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config

Displays the contents of the running configuration.

Syntax

show running-config

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the running configuration. This is the configuration that is currently active on the local device but which is not saved persistently.

This command is supported only on the local device.

Enter **show running-config ?** to display the list of available configuration entries.

Examples

The following command example displays the contents of the running configuration.

```
device# show running-config
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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+
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Must be `0` if the switch does not contain slots.

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# arp 12.1.1.2 0000.0000.0001 interface Ethernet 0/1
```

The following example displays a sample run of the **show running-config arp access-list** option.

```
device# arp access-list acl1
 permit ip host 13.1.1.2 mac host 0000.0000.0002
!
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config event-handler

Displays details of one or all event-handler profiles configured on the device. 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

Command 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 evh2
 trigger 100 raslog NSM-1001
 action python-script vlan.py
!
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config interface port-channel

Displays the configuration of all port channel interfaces on the local switch.

Syntax

show running-config interface port-channel [**number**]

Parameters

number

Specifies a valid port-channel number.

Modes

privileged EXEC mode

Examples

The following example displays configuration information about all port channel interfaces.

```
device# show running-config interface Port-channel
interface Port-channel 20
 insight enable
 no shutdown
!
```

History

Release version	Command history
17s.1.01	This command was introduced.

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
Interface Management 0
Inbound access-list is ipv4 (From User)
Outbound access-list is not set

Interface Ethernet 0/23
   Inbound access-list is std (From User)
   Outbound access-list is not set
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config ip receive

Syntax

show running-config ip receive [**access-group**]

Parameters

access-group
Specifies an IPv4 ACL applied at device-level.

acl-name
Specifies an IPv4 standard or extended ACL.

Modes

Privileged EXEC mode

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config ip route

Displays configuration information for IPv4 routes on this device.

Syntax

show running-config ip route [**static** | **static-route-dest** *ip-address/length* | **static-route-next-vrf-dest** *ip-address/length*]

Parameters

static

Displays information on IPv4 BFD static routes configured for the device.

static-route-dest *ip-address/length*

Displays information for the specified static route destination address. The IP address must be entered in the form A.B.C.D/*length*, where *length* is the address prefix length.

static-route-next-vrf-dest *ip-address/length*

Displays configuration information for the specified next-hop VRF. The IP address must be entered in the form A.B.C.D/*length*, where *length* is the address prefix length.

Modes

Privileged EXEC mode

The following example shows four IPv4 routes are active, including a route to a specific IP address, a route to a virtual interface, a null route, and a route to a physical interface.

```
device# show running-config ip route
ip route 172.161.0.0/16 12.1.1.2
ip route 182.168.2.0/24 ve 2
ip route 182.168.3.0/24 null 0
ip route 192.168.1.0/24 ethernet 0/49
device#
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config ipv6

Displays global IPv6 configurations.

Syntax

show running-config ipv6 access-list [{ **standard** | **extended** } [*acl-name* [**seq** [*seq-number* [*rule-keyword*]]]]]

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
Specifies the IPv6 ACL name.

seq *seq-number*
Specifies a rule. Valid values range from 1 through 4294967290.

rule-keyword
Specifies a rule keyword or operator. For options, type ?.

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 example_1.com
ipv6 nd ra-domain-name user.co.in
ipv6 nd ra-domain-name example_2.com
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config ipv6 access-list

Displays a list of IPv6 ACLs defined on the device, including the rules they contain.

Syntax

show running-config ipv6 access-list [{ **standard** | **extended** } [*acl-name* [**seq** [*seq-number* [*rule-keyword*]]]]]

Parameters

standard
Specifies the standard ACL type.

extended
Specifies the extended ACL type.

acl-name
Specifies the ACL name.

seq *seq-number*
Specifies a rule. Valid values range from 1 through 4294967290.

rule-keyword
Specifies a rule keyword or operator. For options, type ?.

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 device.

```
device# show running-config ipv6 access-list
Interface Management 0
Inbound access-list is 123 (From User)
Outbound access-list is not set

Interface Ethernet 0/23
   Inbound access-list is ext (From User)
   Outbound access-list is not set
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. LDAP is enabled by default and 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.example.com
device#
```

History

Release version	Command history
17s.1.00	This command was added.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config password-attributes

Displays global password attributes.

Syntax

show running-config password-attributes [**admin-lockout**] [**max-lockout-duration**] [**max-retry**] [**min-length**]

show running-config password-attributes character-restriction [**lower** | **numeric** | **special-char** | **upper**]

Parameters

admin-lockout
Displays lockout for admin role accounts.

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.

max-lockout-duration
Displays the maximum number of minutes after which the user account is unlocked. Range is from 0 through 99999. The default is 0, representing an infinite duration.

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 max-lockout-duration 5000
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config radius-server

Displays Remote Authentication Dial-In User Service (RADIUS) server configuration information.

Syntax

show running-config radius-server [**host** { *ip-address* | *hostname* }]

Parameters

host

Causes the display of running configuration information for a specific RADIUS server.

hostname

Specifies a specific RADIUS server in host name format.

ip-address

Specifies a specific RADIUS server in IP address format. Both IPv4 and IPv6 address formats are supported.

Modes

Privileged EXEC mode

Usage Guidelines

When the **host** option is omitted, the **show running-config radius-server** command displays information about all RADIUS servers that are configured on the device.

Command Output

The **show running-config radius-server** command displays the following information:

Output field		Description
radius-server host		RADIUS server identifier.
	auth-port	The user datagram protocol (UDP) port for RADIUS server authentication.
	encryption-level	The encryption level for communication with the RADIUS server.
	key	The text string used as a shared secret between the device and the RADIUS server.
	protocol	The authentication protocol used for communication with the RADIUS server.
	retries	The number of retries allowed to establish a connection with the RADIUS server.
	timeout	The wait time allowed for the RADIUS server response.

Examples

```
device# show running-config radius-server

radius-server host 10.20.51.95 use-vrf mgmt-vrf
   auth-port 1813
   protocol pap
   key sharedsecret
   encryption-level 0
   retries 6
   timeout 10
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

History

Release version	Command history
17s.1.00	This command was introduced.

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 admin desc Administrator
role name user desc User
role name VLANAdmin desc "Manages security CLIs"
role name NetworkAdmin desc "Manages Network CLIs"
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config snmp-server

Shows the user-configured running configuration of the SNMP server on the switch.

Syntax

show running-config snmp-server

Modes

Privileged EXEC mode

Examples

The following command shows the running configuration of the SNMP server on the switch.

```
device# show running-config snmp-server
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Extreme BR-SLX9240 Router"
snmp-server enable trap
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config ssh

Displays the Secure Shell (SSH) status in the running-config.

Syntax

show running-config ssh

Modes

Privileged EXEC mode

Examples

Typical command example:

```
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. SSH is enabled by default and no entry is shown in the running-config when set to default.

Examples

When SSH service is shut down:

```
device# show running-config ssh server
ssh server shutdown
device# show running-config ssh server
ssh server shutdown
ssh server key-exchange dh-group-14
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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-utilization default_system_utilization_statistics
  profile interface default_interface_statistics
  use-vrf mgmt-vrf
  encoding json
  activate
!
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.03	This command was enhanced for the **use-vrf** and **encoding** commands.

show running-config telemetry profile

Displays the configuration settings for one or all telemetry profiles.

Syntax

show running-config telemetry profile [**enhanced-queue-discard-pkts** | **event** | **interface** | **lldp** | **pbr** | **queue** | **system-utilization**]

Modes

Privileged EXEC mode

Parameters

enhanced-queue-discard-pkts
Displays a subset of the data highlighting discarded packet information.

event
Displays configuration information for the **event** profile-type.

interface
Displays configuration information for the **interface** profile-type.

lldp
Displays configuration information for the **lldp** profile-type.

pbr
Displays configuration information for the **pbr** (policy-based routing) profile-type.

queue
Displays configuration information for the current telemetry profile queue.

system-utilization
Displays configuration information for the **system-utilization** profile-type.

Command 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

The following example is the basic command.

```
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 ethernet all
  add out-pkts
  add in-pkts
  …
  add out-discards
  add in-discards
!
```

The following example specifies the **enhanced-queue-discard-pkts** profile-type.

```
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 ethernet all
add discard-pkts
```

The following example specifies the **queue** profile-type.

```
device# show running-config telemetry profile queue
telemetry profile queue default_queue_statistics
interval 240
interface ethernet all
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
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.00	Support was added for the **enhanced-queue-discard-pkts** and **queue** profile-types.
18s.1.02	Support was added for the **event**, **lldp**, and **pbr** profile-types.

show running-config telemetry server

Displays the current configuration of the telemetry server.

Syntax

show running-config telemetry server

Parameters

use-vrf *vrf-name*

(Not supported) Specifies all VRFs or one VRF.

Modes

Privileged EXEC mode

Usage Guidelines

The basic command displays configuration information only for mgmt-vrf.

Examples

The following example is the basic command.

```
device# show running-config telemetry server

telemetry server
  transport ssl
  port <port_number>
  activate
!
```

History

Release version	Command history
17s.1.00	This command was introduced.

show running-config tvf-domain

Displays the running configuration of all defined Transparent VLAN Flooding (TVF) domains or of specified domains.

Syntax

show running-config tvf-domain [*tvf-domain-id*]

Parameters

tvf-domain-id

Specifies the ID of the TVF domain. Valid values are from 1 through 4096. To specify a range of domains, insert a hyphen (-) between the beginning and ending integers (for example, 5-16). To specify individual domains and ranges of domains, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas.

Modes

Privileged EXEC mode

Examples

The following command displays the names of all defined TVF domains.

```
device# show running-config tvf-domain
tvf-domain 1
description Sample TVF domain
!
tvf-domain 2
!
tvf-domain 3
!
tvf-domain 4
!
tvf-domain 5
!
```

History

Release version	Command history
17s.1.01	This command was introduced.
18s.1.00	This command was modified to display TVF-domain descriptions.

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. Values are 0 through 7. 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 "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role admin desc Administrator
username user password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role user desc User
```

The following example displays a specific user account.

```
device# show running-config username admin

username admin password "BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 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 jsmith access-time 0000
username user access-time ""
username user1 access-time 1700
```

History

Release version	Command history
17s.1.00	This command was introduced.

show sflow

Displays sFlow configuration information and statistics.

Syntax

show sflow {**interface ethernet** *slot* **/** *port* | **all** }

Command Default

sFlow is disabled on all interfaces.

Parameters

all

Displays all sFlow information and statistics.

interface

Filters by interface.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

The following example displays all sFlow statistics.

```
device# show sflow all

sFlow services are:                                                    enabled
Global default sampling rate:                                        2048 pkts
Global default counter polling interval:                             20 secs
Collector server address                              Vrf-Name      Sflow datagrams sent
-------------------------------------------------------------------------------
10.10.10.100:6343
                  default-vrf                    0
20.20.20.100:6343
                      mgmt-vrf                       0
```

The following example displays sFlow statistics for a specific interface.

```
device# show sflow interface ethernet 0/1

Port based sflow services are:         enabled
Flow based sflow services are:         disabled
Configured sampling rate:              2048 pkts
Actual sampling rate:                  2048 pkts
Counter polling interval:              20 secs
Port backoffThreshold :                800
Sflow samples collected:               0
Counter samples collected :            0
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The PVST+ and R-PVST+ protocols are supported. The PVST and R-PVST protocols—proprietary to Cisco—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 0/24      DES   FWD  2000       128   P2P               No
Eth 0/32      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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ssh client status

Displays the current Secure Shell (SSH) client key-exchange status.

Syntax

show ssh client status

Modes

Privileged EXEC mode

Examples

When SSH server is enabled:

```
device# show ssh client status
SSH client status: Enabled
device#
```

History

Release version	Command history
17s.1.00	This command was introduced.

show ssh server status

Displays the current Secure Shell (SSH) server key-exchange status.

Syntax

show ssh server status

Modes

Privileged EXEC mode

Examples

When SSH server is enabled:

```
device# show ssh server status
SSH server status: Enabled
device#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
root enable
clock timezone Etc/GMT
hardware
 profile tcam default
 profile route-table default maximum_paths 8
 system-mode default
!
http server use-vrf default-vrf
http server use-vrf mgmt-vrf
logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
logging syslog-client localip CHASSIS_IP
switch-attributes chassis-name SLX9240
switch-attributes host-name cedar-spine-2
no support autoupload enable
support ffdc
resource-monitor cpu enable threshold 90 action raslog
resource-monitor memory enable threshold 100 action raslog
resource-monitor process memory enable alarm 1000 critical 1200
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr " SLX 9240"
snmp-server enable trap
system-monitor fan threshold marginal-threshold 1 down-threshold 2
system-monitor fan alert state removed action raslog
system-monitor power threshold marginal-threshold 1 down-threshold 2
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
<output truncated>
```

History

Release version	Command history
17s.1.00	This command was introduced.

show startup-database

Displays the startup database information.

Syntax

show startup-database

Modes

Privileged EXEC mode

Usage Guidelines

Enter **show startup-database ?** to display the list of available database entries.

Examples

To display the logging configuration in the startup database:

```
device# show startup-db logging
logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
logging syslog-client localip CHASSIS_IP
```

History

Release version	Command history
17s.1.00	This command was introduced.

show statistics access-list

For a given network protocol and inbound/outbound direction, displays ACL statistical information. You can show statistics for a specified ACL or only for that ACL on a specified interface. You can also display statistical information for all ACLs bound to a specified device interface, VLAN or VE. You can also display statistical information for IPv4 or IPv6 receive-path ACLs.

Syntax

show statistics access-list interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id* | **vlan** *vlan_id* } { **in** | **out** }

show statistics access-list { **ip** | **ipv6** } *name* **interface** [**ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id*] { **in** | **out** }

show statistics access-list mac *name* **interface** [**ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan_id*] { **in** | **out** }

show statistics access-list global { **ip** | **ipv6** }

Parameters

interface
Filter by interface.

ethernet
Specifies a physical Ethernet interface.

slot
Specifies a valid slot number.

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.

in | **out**
Specifies the ACL binding direction (incoming or outgoing).

ip | **ipv6** | **mac**
Specifies the network protocol.

name
Specifies the ACL name.

global
Specifies IPv4 or IPv6 receive-path traffic.

Modes

Privileged EXEC mode

Usage Guidelines

Statistics are displayed only for rules that contain the **count** keyword.

Command Output

The **show statistics access-list** command displays the following information:

Output field	Description
Uncount	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 0/8 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 specified interface. The ACL named ipv6-std-acl is applied on interface 0/1 to filter incoming routed traffic only.

```
device# show statistics access-list interface ethernet 0/1 in
ipv6 routed access-list ipv6-std-acl on Ethernet 0/1 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 specified 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show statistics bridge-domain

Displays statistics for the bridge domains.

Syntax

show statistics bridge-domain [*bd-id*]

Parameters

bd-id

Specifies the bridge domain ID.

Modes

Privileged EXEC mode

Usage Guidelines

show statistics bridge-domain *bd- id*

Command Output

The **show statistics bridge-domain** command displays the following information:

Field	Description
BD Index	The bridge domain whose counter statistics are displayed.
RxPkts	The number of packets received on the bridge domain.
RxBytes	The number of bytes received on the bridge domain.
TxPkts	The number of packets transmitted on the bridge domain.
TxBytes	The number of bytes transmitted on the bridge domain.

Examples

The following example displays statistics for all bridge domains.

```
device# show statistics bridge-domain
Bridge-Domain Statistics
BD Index      Rx Pkts             Rx Bytes            Tx Pkts             Tx Bytes
50            0                   0                   0                   0
```

History

Release version	Command history
17r.1.00	This command was introduced.

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

show statistics vlan *vlan- id*

Command 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 Statistics
Vlan Index    Rx Pkts             Rx Bytes             Tx Pkts             Tx Bytes
1             183243862           2580676119971        364658174           211609669029
5             8942910             5527117892           8942910             5527117892
6             8942910             5526859043           8942910             5526859043
7             8942910             5526518757           8942910             5526518757
8             8942910             5527588431           8942910             5527588431
9             8942910             5526423699           8942910             5526423699
```

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 0/1       821729          821729           95940360        95940360
eth 0/2       884484          885855           95969584        95484555
po  1        8884            8855              9684            9955
```

History

Release version	Command history
17s.1.00	This command was introduced.

show storm-control

Displays all BUM (broadcast, unknown unicast and multicast)-related configurations in the system.

Syntax

show storm-control [**broadcast** | **multicast** | **unknown-unicast**] [**interface** { **ethernet** } *0/port*]

Parameters

storm-control
Displays all BUM-related configurations in the system.

broadcast
Displays all BUM-related configurations in the system for the broadcast traffic type.

multicast
Displays all BUM-related configurations in the system for the multicast traffic type.

unknown-unicast
Displays all BUM-related configurations in the system for the unknown-unicast traffic type.

interface ethernet *0/port*
Displays the information for the specified interface. Specifies a valid slot and port number. The slot number must be 0, because the switch does not contain slots.

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 specified interface.

Examples

To display storm control information for broadcast traffic on an Ethernet interface:

```
device# show storm-control broadcast interface ethernet 0/3

Interface    Type          rate (Mbps)  conformed    violated      total
Eth 0/3      broadcast     100,000      12500000000  12500000000   25000000000
```

To display storm control information for all traffic on an Ethernet interface.

```
device# show storm-control interface ethernet 0/3

Interface    Type             rate (Mbps)  conformed   violated    total
Eth 0/3      broadcast        100,000      12500000000 12500000000 25000000000
Eth 0/3      unknown-unicast  100,000      12500000000 12500000000 25000000000
Eth 0/3      multicast        100,000      12500000000 12500000000 25000000000
```

To display storm control information for all traffic in the system:

```
device# show storm-control

Interface   Type             rate (Mbps)  conformed   violated    total
Eth 0/3      broadcast        100,000      12500000000 12500000000 25000000000
Eth 0/3      unknown-unicast  100,000      12500000000 12500000000 25000000000
Eth 0/3      multicast        100,000      12500000000 12500000000 25000000000
Eth 0/7      broadcast        100,000      12500000000 12500000000 25000000000
Eth 0/5      broadcast        100,000      12500000000 12500000000 25000000000
Eth 0/9      unknown-unicast  100,000      12500000000 12500000000 25000000000
```

To display storm control information for all broadcast traffic the system:

```
device# show storm-control broadcast

Interface    Type             rate (Mbps)  conformed   violated    total
Eth 0/1      broadcast        100,000      12500000000 12500000000 25000000000
Eth 0/2      broadcast        100,000      12500000000 12500000000 25000000000
Eth 0/3      broadcast        100,000      12500000000 12500000000 25000000000
```

History

Release version	Command history
17s.1.00	This command was introduced.

show support

Displays a list of core files on the switch.

Syntax

show support

Command Default

Displays information for the local switch.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

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!
```

History

Release version	Command history
17s.1.00	This command was introduced.

show system

Displays hardware and software system information.

Syntax

show system

Modes

Privileged EXEC mode

Examples

To display the system information:

```
device# show system
Stack MAC                     : 60:9c:9f:b1:0b:00

  -- UNIT 0 --
Unit Name                     : F115
Ethernet Port(s)              : 54
Up Time                       : up 2 days 23:55
Current Time                  : 19:03:43 GMT
SLX-OS Version                : 17s.1.00_bfd_fix
Jumbo Capable                 : yes
Burned In MAC                 : 60:9C:9F:B1:0B:AA
Management IP                 : 10.20.234.115
Management Port Status        : UP

  -- Power Supplies --
PS1 is OK
PS2 is faulty

  -- Fan Status --
Fan 1 is Ok, speed is 5857 RPM
Fan 2 is Ok, speed is 5677 RPM
Fan 3 is Ok, speed is 5677 RPM
Fan 4 is Ok, speed is 5677 RPM
Fan 5 is Ok, speed is 5857 RPM
Fan 6 is Ok, speed is 5857 RPM
```

History

Release version	Command history
17s.1.00	This command was introduced.

show system internal dcm

Displays distributed configuration management (DCM) information in the system.

Syntax

show system internal dcm { **clients** | **last-config-time xpaths** | **memstat** [**detail**] | **message-stat all** | **object-stat all** }

show system internal dcm message details config service *service-number* { **off** | **on** }

show system internal dcm service [**details**] *service-number*

show system internal dcm vlan { **port-vlans** | **provisioned-vlans** | **vlans-with-ivid** }

Parameters

clients
Displays connected clients.

last-config-time xpaths
Displays last configuration-time xpaths.

memstat
Displays DCM memory statistics.

detail
Displays detailed DCM memory statistics.

message-stat all

ATTENTION
Running this command can use significant system resources.

Displays a summary of all DCM messages.

object-stat all
Displays a summary of DCM object statuses.

message details config service *service-number*
Turns on and off a DCM message-history dump for a specified service number. The default is **off**.

off
Turns off the specified message-history dump.

on
Turns on the specified message-history dump.

service
Displays detailed or summary information for a DCM service.

details
Displays detailed information. If this option is not specified, displays summary information.

service-number
Specifies a service number.

vlan

Displays VLAN-related details.

port-vlans

Displays port-VLAN associations.

provisioned-vlans

Displays provisioned VLANs.

vlans-with-ivid

Displays VLANs associated with IVID.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Examples

The following command displays DCM connected clients.

```
device# show system internal dcm clients
Client Name
------------
DPoD_License0
IGMP0
InterDcmCcmClient_ccm
LldpDCMClient0
SMD
Sflow0
UdldDCMClient0
WaveClient010.20.234.1159810
arp0
bfdd0
bgp0
ctpd0
dauthd0
eld0
fibagt_p00
iphelpd0
l2agt_p00
l2sys0
lacp0
mc_agt.0.0
mc_hms0
mcast_ss0
mct0
mstp0
nsm0
ospf0
ospf60
pcap0
pem0
pim0
ptp0
qos0
radv0
rmon0
rps0
rtm0
snmp0
srm0
ssm0
tnl0
tnlagt_p00
vrrp0
```

The following command displays a summary of DCM object statuses.

```
device# show system internal dcm object-stat all
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'SMANLocalObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'ZTP Local Manager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service :
'sysdiagOperationalDataObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'SysmgrLocalObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service :
'SysmgrOperationalDataObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service :
'OverlayPolicyGlobalObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service :
'OverlayPolicyLocalObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'TelemetryLocalObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'Confd Gateway Interface'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'ConfdMaapiObjectManager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'Confd Async Object Manager'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
INFO   : Tue Mar  7 19:25:50 2017 : Leaked Object Summary For Service : 'Cluster interface'
SUCCESS: Tue Mar  7 19:25:50 2017 : NO Object Leaks Found.
SUCCESS: Tue Mar  7 19:25:50 2017 : SUCCEEDED to dump object leaks
```

History

Release version	Command history
17s.1.00	This command was introduced.

show system internal nsm

Displays network service module (NSM) information in the system.

Syntax

show system internal nsm { **gvlan** [*vlan-id*] | **ivid** [*vlan-id*] | **vrbid** }

Parameters

gvlan

Displays global-VLAN (GVLAN) information.

vlan-id

Displays GVLAN information for a specified VLAN.

ivid

Displays information for VLANs associated with IVIDs.

vlan-id

Displays GVLAN information for a specified VLAN.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Examples

The following example displays information for IVIDs provisioned to VLAN 1.

```
device# show system internal nsm ivid 1

VID-IVID Mapping     :  Uniform

Total # of IVIDs provisioned to Vlans:   513
Total # of free IVIDs :   7543

GVLAN       IVID        # of Ifs
1           1           7
```

The following example is sample output for the **show system internal nsm gvlan** option.

```
device# show system internal nsm gvlan

Vfab enable state : disabled
Vfab en read status, rc : 0 0
Vfab en stage 0, status 0, dis stage 0, status 0

Total # of Vlans configured: 513

Total # of Vlans provisioned: 513

GVLAN       IVID        # of Ifs
1           1           7
101         101         1
102         102         1
103         103         1
104         104         1
105         105         1
106         106         1
107         107         1
108         108         1
109         109         1
110         110         1
111         111         1
112         112         1
113         113         1
114         114         1
115         115         1
116         116         1
117         117         1
118         118         1
119         119         1
120         120         1
121         121         1
122         122         1
<output truncated>
```

History

Release version	Command history
17s.1.00	This command was introduced.

show system internal nsx

Displays state information related to the NSX controller.

Syntax

show system internal nsx export-vlan-cache

show system internal nsx { **locator-cache** | **lswitch-cache** } [**count**]

Parameters

export-vlan-cache
Displays the export-VLAN cache.

locator-cache
Displays the physical-locator cache.

count
Displays only the number of cache entries.

lswitch-cache
Displays the logical-switch cache.

count
Display only the number of cache entries.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Examples

The following example shows a sample output of the **show system internal nsx export-vlan-cache** option.

```
device# show system internal nsx export-vlan-cache
41-42,1011-3010
(2002 vlans)
```

The following example shows a sample output of the **show system internal nsx lswitch-cache** option.

```
device# show system internal nsx lswitch-cache
Logical_Switch UUID                    VNI       GVLAN    ObjectId
================================================================================
38a71eb3-8524-3982-af91-29d66ff7f13b   -1        0     262795638:2203318222851
39dbad3a-0765-3c22-a2c7-257ce8e8c71b   555555    41    262795638:2203318222849
c94fbfd9-6515-3faf-b8ac-3608bcabeb75   6000      42    262795638:2203318222850
(3 entries)
```

The following example shows a sample output of the **show system internal nsx locator-cache** option.

```
device# show system internal nsx locator-cache
Physical_Locator UUID                  Tun ID    ObjectId
================================================================================
62323fc8-8e7f-367e-9592-99d73f065357   61441     7525106:2203318222849
e08bad93-30f1-35e9-b2c3-808f75e056ce   61442     7525106:2203318222850
(2 entries)
```

History

Release version	Command history
17s.1.00	This command was introduced.

show system internal ovsdb

Displays system information from the ovsdb tables.

Syntax

show system internal ovsdb { **monitors** | **schema** }

show system internal ovsdb table *name* [**count** | **where** *column function value*]

Parameters

monitors
Specifies registered monitors.

schema
Specifies all ovsdb schemas and tables.

table *name*
Specifies an ovsdb table.

count
Specifies the number of rows.

where
Specifies a condition.

column
Specifies a table column.

function
Specifies a function, for example, **=**.

value
Specifies the column value.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Examples

The following example shows a sample output of the **show system internal ovsdb schema** option.

```
device# show system internal ovsdb schema
  Schema: hardware_vtep
 Tables:
    Arp_Sources_Local
    Arp_Sources_Remote
    Global
    Logical_Binding_Stats
    Logical_Router
    Logical_Switch
    Manager
    Mcast_Macs_Local
    Mcast_Macs_Remote
    Physical_Locator
    Physical_Locator_Set
    Physical_Port
    Physical_Switch
    Tunnel
    Ucast_Macs_Local
    Ucast_Macs_Remote
```

The following example shows a sample output of the **show system internal ovsdb table** *name* **where** option.

```
device # show system internal ovsdb table Logical_Switch where tunnel_key=444444
 ===== Row 1 of 1 =====
description          : LS-5000
name                 : 6eaf567f-6129-4125-8fa1-d3e5b8cf946c
tunnel_key           : 444444
_uuid                : 39dbad3a-0765-3c22-a2c7-257ce8e8c71c
_version             : 52e15220-eca6-3b7e-bab9-324d2ea7cef5
```

History

Release version	Command history
17s.1.00	This command was introduced.

show system monitor

Displays the overall switch status and the status of the contributors defined as part of the policy.

Syntax

show system monitor

Modes

Privileged EXEC mode

Examples

The following example displays the status of the local switch.

```
device# show system monitor
** System Monitor Switch Health Report **
               Switch status            : HEALTHY
               Time of Report           : 2017-03-07 19:05:02
               Power supplies monitor   : HEALTHY
               Temperatures monitor     : HEALTHY
               Fans monitor             : HEALTHY
               Flash monitor            : HEALTHY
```

History

Release version	Command history
17s.1.00	This command was introduced.

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-----
```

History

Release version	Command history
17s.1.00	This command was introduced.

show telemetry collector

Displays the status of telemetry collectors.

Syntax

show telemetry collector { **summary** | **name** *collector-name* }

Parameters

summary

Displays a summary of the Telemetry collectors.

name *collector-name*

Displays the information for the designated collector.

Modes

Privileged EXEC mode

Command Output

The **show telemetry collector** command displays the following information:

Output field	Description
Name	The name of the unique collector profile.
IP Address:Port	The IP address and port for the collector profile.
Streaming/Connection Status	The current status of the collector profile.
Profiles Streamed	The telemetry profiles the collector is utilizing.
Interval	The interval setting for the collector profile.
Uptime	The uptime for the collector profile.
Last Streamed	The date and time the collector profile was last streamed.

Examples

Typical summary output.

```
device# show telemetry collector summary

Activated Collectors:
----------------------
Name                    IP Address:Port           Streaming/Connection Status
--------------------    -------------------      ---------------------------
Collector_3333          10.70.12.112:33333         starting_profiles
Collector_4444          10.70.12.112:44444         streaming
Collector_2345          10.70.12.112:33333         streaming_errored
```

Typical output for a specific collector.

```
device# show telemetry collector name kCollector_3333

Telemetry data is streamed to Collector_3333 on IP 10.70.12.112 and port 33333.

Profiles Streamed                     Interval   Uptime      Last Streamed
-------------------                   ---------  ----------  ---------------
default_interface_statistics          120 sec    02/15:32    2017-01-18::22:55:12
default_system_utilization_statistics  300 sec    04/05:44    2017-02-03::05:36:15
!
```

History

Release version	Command history
17s.1.00	This command was introduced.

show telemetry server status

Displays the current status of the telemetry server.

Syntax

show telemetry server status

Modes

Privileged EXEC mode

Command Output

The **show telemetry server status** command displays the following information:

Output field	Description
Client	The name of the unique client profile.
IP Address:Port	The IP address and port for the client profile.
Streaming/Connection Status	The current status of the client profile.
Profiles Streamed	The telemetry profiles the client is utilizing.
Interval	The interval setting for the client profile.
Uptime	The uptime for the client profile.
Last Streamed	The date and time the client profile was last streamed.

Examples

Typical command output.

```
device# show telemetry server status

Telemetry Server running on IP 10.70.12.112 and port 33333, with transport as tcp.

Active Sessions:
----------------
Client            Profiles Streamed                    Interval   Uptime      Last Streamed
------            -----------------                    ---------  ----------  ---------------
ClientIP1/Host1   default_interface_statistics          120 sec    02/15:32    2017-01-18::22:55:12
                  default_system_utilization_statistics  300 sec    04/05:44    2017-02-03::05:36:15

ClientIP2/Host2   default_system_utilization_statistics  300 sec    05/08:36    2017-02-05::09:56:35
!
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show threshold monitor

Displays the current status of environmental thresholds and alerts for interfaces, security, and SFPs.

Syntax

show threshold monitor [**interface all area** | **security area** [**login-violation** | **telnet-violation**] | **sfp all area** [**current** | **rxp** | **temperature** | **txp** | **voltage**]

Parameters

interface all area
Displays status of interface thresholds and alerts.

security area
Displays status of security thresholds and alerts.

login-violation
Displays status of login violations.

telnet-violation
Displays status of Telnet violations.

sfp all area
Displays status of SFP thresholds and alerts.

current
Amount of current supplied to the SFP transceiver.

rxp
Amount of incoming laser power, in microWatts (µW).

temperature
Temperature of the SFP, in degrees Celsius.

txp
Amount of outgoing laser power, in microWatts (µW).

voltage
Amount of voltage supplied to the SFP.

Modes

Privileged EXEC mode

Examples

```
device# show threshold monitor sfp all area temperature
Interface                           Type            Area            Value           Status
Monitoring Status
-------------------------------------------------------------------------------------------------------
---------------
Eth 0/3                             10GSR           Temperature     26 Centigrade   In Range
Monitoring
Eth 0/4                             10GSR           Temperature     24 Centigrade   In Range
Monitoring
```

History

Release version	Command history
17s.1.00	This command was introduced.

show tpvm

Displays status of Third-Party Virtual Machine (TPVM) applications.

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. See the Usage Guidelines.

status

Displays TPVM information.

Modes

Privileged EXEC mode

Examples

To display the current status of TPVM or any errors:

```
device# show tpvm status
```

History

Release version	Command history
18s.1.01	This command was introduced.

show tunnel

Displays information pertaining to a tunnel interface.

Syntax

show tunnel *tunnel-id*

show tunnel brief [*node-id*]

show tunnel replicator *node-id*

show tunnel statistics {*tunnel-id* | **dst-ip** *destination-ip* | **mode** [*gre* | *vxlan*] | **node-id** [*node-id*] | **overlay-gateway** [*overlay-gateway-name*] | **src-ip** *source-ip* }

show tunnel status {*tunnel-id* | **dst-ip** *destination-ip* | **mode** [*gre* | *vxlan*] | **node-id** *node-id* | **overlay-gateway** [*overlay-gateway-name*] | **src-ip** *source-ip* }

Parameters

tunnel-id
Specifies the tunnel ID.

replicator
Displays tunnels to NSX replicators

node-id
Displays from specified nodes

statistics
Displays tunnel statistics.

dst-ip*destination-ip*
Filters by tunnel destination IP address.

mode [*gre* | *vxlan*
Filters by tunnel mode.

node-id *node-id*
Displays from specified nodes.

overlay-gateway [*overlay-gateway-name*
Filters by overlay gateway name.

src-ip *source-ip*
Filters by tunnel source IP address.

Modes

Privileged EXEC Mode

Examples

This example displays tunnel information.

```
device# show tunnel 10
Tunnel 10, mode GRE
Ifindex 0x7c40000a, Admin state up, Oper state up
Source IP 14.101.0.4, Vrf default-vrf
Destination IP 15.10.0.3
Tunnel IP Interface : Ve 501 up
Tunnel TTL 255      Tunnel DSCP 0
Tunnel QosMode PIPE
Keepalive Interval 10000  RetryCount 3 TimeRemaining 27861 msecs
GRE Keep Alive : RX 62      TX 62

Active next hops:
    IP: 13.10.0.3, Vrf: default-vrf
    Egress L3 port: Ve 10, Outer SMAC: 609c.9f0d.4a14
    Outer DMAC: 001b.ed9f.1700
    Egress L2 Port: Unknown, Outer ctag: 0, stag:0, Egress mode: Local
    BUM forwarder: no
```

History

Release version	Command history
17s.1.00	This command was introduced.

show tunnel statistics

Displays tunnel statistics.

Syntax

show tunnel statistics *tunnel-Id* **mode** [**gre** | **vxlan**]

show tunnel statistics node-id *node-Id*

show tunnel statistics overlay-gateway *overlay-gatway-name*

show tunnel statistics src-ip *source-ip*

Parameters

tunnel-Id
Filters by the tunnel ID.

mode
FIlters by tunnel mode.

gre
Specifies GRE tunnels.

node-id *node-Id*
Displays from the specified node ID.

overlay-gateway *overlay-gatway-name*
Filter by overlay gateway name.

src-ip *source-ip*
Filter by tunnel source IP address.

Modes

Privileged EXEC Mode

Examples

This example displays tunnel statistics filtered by the tunnel ID.

```
device# show tunnel statistics 11
Tnl ID   RX packets      TX packets      RX bytes        TX bytes
======== =============== =============== =============== ================
11       0               10               (NA)            640
```

This example displays tunnel statistics filtered by tunnel mode.

```
device# show tunnel statistics mode gre
Tnl ID   RX packets      TX packets      RX bytes        TX bytes
======== =============== =============== =============== ================
10       0               10               (NA)            640
11       0               20               (NA)            1280
12       0               50               (NA)            22000
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

show version

Displays the current firmware version.

Syntax

show version [**all-partitions**] [**brief**]

Parameters

all-partitions

Displays firmware information for both the active and the standby partitions. For each module, both partitions are displayed.

brief

Displays a brief version of the firmware information.

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:

- Network Operating System 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
- Host Version—The Linux host version.
- Host Kernel—The Linux kernel version
- Control Processor—The control processor model and memory

Examples

To display the firmware version information for all partitions:

```
device# show version all-partitions

SLX-OS Operating System Software
SLX-OS Operating System Version: 17s.1.00
Copyright (c) 2017-2018 Extreme Networks, Inc.
Firmware name:      17s.1.00_bfd_fix
Build Time:         23:24:03 Mar  3, 2017
Install Time:       18:54:34 Mar  4, 2017
BIOS Version:       5.11 built on 07/12/2016
ONIE Version:       2016.05.09-dirty (17s.1.00nhess_dv_drop11_merge_161013_1611)
Diag Version:       1.2.2.42 (17s.1.00nhess_dv_drop11_merge_161013_1611)
Kernel:             2.6.34.6
Host Version:       Ubuntu 14.04 LTS
Host Kernel:        Linux 3.14.17

Control Processor:   QEMU Virtual CPU version 2.0.0

System Uptime:   3days 1hrs 29mins 0secs

Slot    Name    Primary/Secondary Versions                          Status
-------------------------------------------------------------------------
SW/0    SLX-OS  17s.1.00_bfd_fix                                   ACTIVE*
                17s.1.00_bfd_fix
```

To display the firmware for all partitions in the brief view:

```
device# show version all-partitions brief

Slot    Name    Primary/Secondary Versions                          Status
-------------------------------------------------------------------------
SW/0    SLX-OS  17s.1.00_bfd_fix                                   ACTIVE*
                17s.1.00_bfd_fix
```

History

Release version	Command history
17s.1.00	This command was introduced.

show vlan

Displays information about one or more VLAN interfaces.

Syntax

show vlan [*vlan_id* | **brief** [**provisioned** | **unprovisioned**] | **classifier**]

Parameters

vlan_id
Specifies the VLAN interface to display.

brief
Displays VLAN information for all interfaces including static and dynamic.

classifier
Displays all VLAN classification information.

provisioned
Displays provisioned VLANs.

unprovisioned
Displays unprovisioned VLANs.

Modes

Privileged EXEC mode

Examples

The following example displays information about an 802.1Q VLAN:

```
device# show vlan 1

VLAN     Name            State   Ports
                                 (u)-Untagged, (t)-Tagged
                                 (c)-Converged
======= ================ ======= ================================
1       default          ACTIVE  Eth 0/0(t)
                                 Eth 0/8(t)
                                 Po 1(t)
```

The following example shows all VLANs that are configured, provisioned (active) and unprovisioned (inactive):

```
device# show vlan brief

Total Number of VLANs configured:    6
Total Number of VLANs unprovisioned: 0
Total Number of VLANs provisioned:   6
VLAN        Name         State   Ports             Classification

(T)-Transparent                 (t)-Tagged
(R)-RSPAN                       (c)-Converged
 ========================================
300         vlan300      INACTIVE    Eth 0/1(t)
5000(T)     vlan5000     ACTIVE      Eth 0/2(t)  ctag 50, 60, 100-200
                                     Eth 0/3(t)  ctag 50, 60, 100-200
5500(T)     vlan5500     ACTIVE      Eth 0/4(t)  ctag 1, 1002, 4093, 4095
5800        vlan5800     ACTIVE      Eth 0/5(t)  ctag 800
6000(T)     vlan6000     ACTIVE      Eth 0/1(t)
```

The following example shows only provisioned VLANs:

```
device# show vlan brief provisioned
Total Number of VLANs configured:    8
Total Number of VLANs unprovisioned: 3
Total Number of VLANs provisioned:   5
VLAN        Name         State   Ports             Classification

                                 (t)-Tagged
(R)-RSPAN                        (c)-Converged
 ========================================
1           default      ACTIVE  Eth 0/1(c)
5000        VLAN5000     ACTIVE  Eth 0/1(t)       ctag 100
                                 Eth 0/2(u)       ctag 200
                                 Eth 0/3(u)
                                 Eth 0/4(u)       mac 0004.0004.0004
6000        VLAN6000     ACTIVE  Eth 0/1(t)       ctag 300
                                 Eth 0/2(u)       mac 0002.0002.0002
                                 Eth 0/3(u)       mac-group 1
                                 Po 10(t)         ctag 300
7000        VLAN7000     ACTIVE  Eth 0/1 (t)      ctag 400
                                 Eth 0/2 (u)      mac 0006.0006.0006
                                 Eth 0/3 (u)      mac-group 2
1002(F)     VLAN1002     ACTIVE  Eth 0/5(t)
                                 Eth 0/6(t)
```

The following example shows only unprovisioned VLANs:

```
device# show vlan brief unprovisioned
Total Number of VLANs configured:      8
Total Number of VLANs unprovisioned: 3
Total Number of VLANs provisioned:     5
VLAN              Name          State                  Ports

(R)-RSPAN                                                              (c)-Converged
======== ================ ======= ======
2000           VLAN2000      INACTIVE(unprovisioned)
4000           VLAN4000      INACTIVE(unprovisioned)
8000           VLAN8000      INACTIVE(unprovisioned)
```

History

Release version	Command history
17s.1.00	This command was introduced.

show vlan brief

Displays basic information about switch VLAN interfaces. You can 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

Command 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.
Ports	Displays the ports on which the VLAN is applied.
Classification	(Available only for provisioned.)
Configuration Source	Displays whether source is static or dynamic (including for Endpoint Tracking)

Examples

The following example shows all VLANs that are configured, provisioned (active) and unprovisioned (inactive). VLAN 5800 was assigned the name "marketing."

```
device# show vlan brief

Total Number of VLANs configured:    6
Total Number of VLANs unprovisioned: 0
Total Number of VLANs provisioned:   6
VLAN        Name         State   Ports             Classification

(T)-Transparent                  (t)-Tagged
(R)-RSPAN                        (c)-Converged
 ========================================
300         vlan300      INACTIVE    Eth 0/1(t)
5000(T)     vlan5000     ACTIVE      Eth 0/2(t)    ctag 50, 60, 100-200
                                     Eth 0/3(t)    ctag 50, 60, 100-200
5500(T)     vlan5500     ACTIVE      Eth 0/4(t)    ctag 1, 1002, 4093, 4095
5800        marketing    ACTIVE      Eth 0/5(t)    ctag 800
6000(T)     vlan6000     ACTIVE      Eth 0/1(t))
```

The following example shows endpoint tracking enabled.

```
device# show vlan brief
Total Number of VLANs configured    : 2
VLAN             Name       State       Ports           Classification   Configuration
(R)-RSPAN                               (u)-Untagged                     Source
                                        (t)-Tagged
================ ========== ================================ ================  =============
1                default    ACTIVE      Eth 0/2(t)                        Static
                                        Eth 0/1(t)                        Static
10               VLAN0010   ACTIVE      Eth 0/2(t)
Static

30               VLAN0030   ACTIVE      Eth 0/22(t)                       Dynamic(Endpoint Tracking)
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.01a	This command was modified to support endpoint tracking.

show vlan classifier

Displays information about a specific VLAN classifier group.

Syntax

show vlan classifier [**group** *number* | **interface** *group-number* | **interface port-channel** *number* | **rule** *number* | **interface ethernet** *slot/port*]

Parameters

group *number*
Specifies the VLAN classifier group number. Valid values range from 1 through 16.

interface *group number*
Specifies the VLAN classifier interface group number. Valid values range from 1 through 16.

interface port-channel *number*
Specifies the VLAN classifier port-channel number. Valid values range from 1 through 63.

rule *number*
Specifies the VLAN classifier rule number. Valid values range from 1 through 256.

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.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about all configured VLAN classifier groups or a specific VLAN interface group.

If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is specified, a specific configured VLAN classifier group is shown.

History

Release version	Command history
17s.1.00	This command was introduced.

show vlan private-vlan

Displays information about private VLANs.

Syntax

show vlan private-vlan

Modes

Privileged EXEC mode

Examples

Typical command output display:

```
device# show vlan private-vlan

Primary   Secondary Type      Ports          Classification
=======   =======   ======    ===========    ==============================
6000                primary   Eth 0/1(t)     ctag 10
                              Eth 0/2(t)     ctag 10
6000      6001      isolated  Eth 0/3(t)     ctag 11
                              Eth 0/4(t)     ctag 11
6000      6002      community Eth 0/5(t)     ctag 12
                              Eth 0/6(t)     ctag 12
6000      6003      community Eth 0/7(t)     ctag 13
                              Eth 0/8(t)     ctag 13
```

History

Release version	Command history
17s.1.00	This command was introduced.

show vlan rspan-vlan

Displays information about remote SPAN VLANs.

Syntax

show vlan rspan-vlan

Modes

Privileged EXEC mode

Examples

```
device# show vlan rspan-vlan
Total Number of VLANs configured    : 3
Total Number of VLANs provisioned   : 2
Total Number of VLANs unprovisioned : 1
VLAN          Name        State                      Ports        Classification
============= =========== ======================     ============ ======
6000(R)       VLAN6000    INACTIVE(member port down) Eth 0/2(t)   ctag 121
6001(R)       VLAN6001    INACTIVE(member port down) Eth 0/3(t)   ctag 555
```

History

Release version	Command history
17s.1.00	This command was introduced.

show vrf

Displays Virtual Routing and Forwarding (VRF) configuration information.

Syntax

show vrf [*vrf-name* | **detail** | **interface** *interface*]]

Parameters

vrf-name

Specifies a named VRF. For the default VRF, enter **default-vrf**.

detail

Displays detailed information for all VRFs configured.

interface *interface*

Displays VRF information for an interface.

Modes

Privileged EXEC mode

Examples

The following 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
```

The following 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
```

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* | **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. The slot number must be 0 if the switch does not contain slots.

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
```

The following example displays information about the configured values for the Owner Priority and Owner Track-Priority. In this example, owner preemption is enabled because the value of owner priority is set to 250 (owner priority is 255 by default), and interfaces are to be tracked on the owner device with a configured priority of 50 if the interface goes down.

```
device# show vrrp

Total number of VRRP session(s)    : 1

VRID 1
  Interface: Ve 100;  Ifindex: 1207959652
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Initialize
  Session Master IP Address:
  Virtual IP(s): 10.1.1.100
  Configured Priority: unset (default: 100); Current Priority: unset
  Configured Owner Priority: 250; Owner Track-Priority: 50
  Advertisement interval: 2 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)
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========
  Statistics:
    Advertisements: Rx: 0, Tx: 0
    Gratuitous ARP: Tx: 0
```

History

Release version	Command history
17s.1.00	This command was introduced.

Commands Shu - Z

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

The following example disables an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# shutdown
```

The following example enables an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# no shutdown
```

The following example disables a port-channel interface.

```
device# configure terminal
device(config)# interface port-channel 20
device(config-Port-channel-20)# shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

site

Creates a remote Layer 2 extension site in a VXLAN overlay gateway context and enables VXLAN overlay gateway 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

VXLAN 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, and the administrative state.

Use the **no site** command with a specified name to remove the tunnel that corresponds to the site. Once 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 7 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 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.
mac-learning protocol bgp	Changes the default MAC learning on a tunnel from Layer 2 to BGP MAC learning.
shutdown	Administratively shuts down tunnels to a VXLAN overlay gateway site.

Examples

The following example creates a VXLAN overlay gateway site and enter VXLAN overlay gateway site configuration mode.

```
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-site-mysite)#
```

History

Release version	Command history
17s.1.01	This command was introduced.

snmp-server access-enable vrf

Disables SNMP traps for the interface link status change.

Syntax

snmp-sever access-enable vrf { **all** | **vrf 1** [*vrf-2 ...vrf-4default-vrf mgmt-vrf*]}

no snmp-sever access-enable vrf { **all** | **vrf 1** [*vrf-2 ...vrf-4default-vrf mgmt-vrf*]}

By default, the SNMP server access is enabled for all VRF instances.

Parameters

all

Enables SNMP access to all VRF instances.

vrf-1 [*vrf-2 ...vrf-4default-vrf mgmt-vrf*

Enable access to listed VRF instances. Each VRF instance is a string of maximum number of 32 characters. The maximum number of VRF instances that can be enabled for an SNMP server is 6.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove SNMP server access from all or listed VRF instances.

The maximum number of VRFs (including the default VRF and mgmt VRF) supported for this feature is 6 .

NOTE

- You cannot enable access to specific VRF instances in the default configuration.
- You cannot enable access to all VRF instances when a list of VRF instances are listed in an existing configuration.

During a software upgrade, SNMP server access is enbled for all VRFs instances.

Examples

The following example enables SNMP server access for VRF 1

```
device# configure terminal
device(config)# snmp-server access-enable vrf vrf-1
```

The following example disables SNMP server access for VRF 1

```
device# configure terminal
device(config)# no snmp-server access-enable vrf vrf-1
```

History

Release version	Command history
18s.1.01	This command was introduced.

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* [**groupname** *name*]

no snmp-server community *string* [**groupname** *name*]

Parameters

string
Specifies the community name string. Enter an alphanumeric string with 2 to 16 characters.

groupname *name*
Specifies the group name associated with the community name.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove the 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# configure terminal
device(config)# snmp-server community public groupname user
```

History

Release version	Command history
17s.1.00	This command was introduced.

snmp-server contact

Sets the SNMP server contact string.

Syntax

snmp-server contact *string* [**location** *string*] [**sys-descr** *string*]

no snmp-server contact *string* [**location** *string*] [**sys-descr** *string*]

Command Default

The default contact string is Field Support.

The default location string is End User Premise.

The default system description string is "Extreme BR-SLX9140 Switch" or "Extreme BR-SLX9240 Switch".

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.

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.

sys-descr *string*

Specifies the Management Information Base (MIB-2) object identifier (OID) system description. 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# configure terminal
device(config)# snmp-server contact "Operator 12345"
```

History

Release version	Command history
17s.1.00	This command was introduced.

snmp-server context

Maps the context name in an SNMPv3 packet protocol data unit (PDU) to the name of a Virtual 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*]

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 also 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.

ATTENTION
SNMP SET requests work only on the default VRF.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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# configure terminal
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# configure terminal
device(config)# no snmp-server engineid local
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** } [**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

no snmp-server group *groupname* { **v1** | **v2c** | **v3** } [**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

Parameters

groupname
Specifies the name of the SNMP group to be created.

v1 | **v2c** | **v3**
Specifies the version of SNMP.

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.

Examples

The following example creates SNMP server group entries for SNMPv3 user group.

```
device# configure terminal
device(config)# snmp-server group group1 v3 read myview write myview notify myview
device(config)# snmp-server group group2 v3 read all write all notify all
device(config)# snmp-server group group3 v3
```

The following example removes the configured SNMP server groups.

```
device# configure terminal
device(config)# no snmp-server group test1 v3
device(config)# no snmp-server group TEST1 v3 read myview write myview
device(config)# no snmp-server group TEST2 v3 read all write all notify all
```

History

Release version	Command history
17s.1.00	This command was introduced.

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-vrf vrf-name**]

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**]

Parameters

{ **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 for both v1/v2 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").

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 (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** *string* **version 2c** command brings version 2c down to version 1.

The **no snmp-server host** *host* **community-string** *string* command removes the SNMP server host from the device configuration altogether.

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 host1.example.com associated with community "public." The trap host receives traps from the configured device.

```
device# configure terminal
device(config)# snmp-server host host1.example.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# configure terminal
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# configure terminal
device(config)# snmp-server host 10.23.23.45 public severity-level info
```

The following example resets the severity level to None.

```
device# configure terminal
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# configure terminal
device(config)# snmp-server host 10.24.61.10 public use-vrf myvrf
```

History

Release version	Command history
17s.1.00	This command was introduced.

snmp-server location

Sets the SNMP server location string.

Syntax

snmp-server location *string* [**contact** *string*] [**sys-descr** *string*]

no snmp-server location *string* [**contact** *string*] [**sys-descr** *string*]

Command Default

The default location string is End User Premise.

The default contact string is Field Support.

The default system description string is "Extreme BR-SLX9140 Switch" or "Extreme BR-SLX9240 Switch".

Parameters

contact *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.

sys-descr *string*

Specifies the Management Information Base (MIB-2) object identifier (OID) system description. 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# configure terminal
device(config)# snmp-server location "Building 3 Room 214"
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*

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 "inetCidrRouteTable". 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# configure terminal
device(config)# no snmp-server mib community-map public context mycontext
```

History

Release version	Command history
17s.1.00	This command was introduced.

snmp-server sys-descr

Sets the Management Information Base (MIB-2) object identifier (OID) system description.

Syntax

snmp-server sys-descr *string* [**contact** *string*] [**location** *string*]

no snmp-server sys-descr *string* [**contact** *string*] [**location** *string*]

Command Default

The default system description string is "Extreme BR-SLX9140 Switch" or "Extreme BR-SLX9240 Switch".

The default contact string is Field Support.

The default location string is End User Premise.

Parameters

string
Specifies the system description. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

contact *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.

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 system description OID to "Extreme Cluster device".

```
device# configure terminal
device(config)# snmp-server sys-descr "Extreme Cluster device"
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* [**groupname** *group-name*] [**auth** { **md5** | **sha** | **noauth** }] [**auth-password** *string* [**encrypted**]] [**priv** { **DES** | **AES128** | **nopriv** }] [**priv-password** *string* [**encrypted**]]

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.

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.

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 also 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 this command to do one of more of the following:

- Remove the specified user and all entities associated with it
- Remove the groupname from the user

Examples

The following example configures a basic authentication policy.

```
device# configure terminal
device(config)# snmp-server user user_01 groupname snmpadmin auth md5 auth-password user123 priv AES128
priv-password user456
```

The following example configures plain-text passwords.

```
device# configure terminal
device(config)# snmp-server user snmpadmin1 auth md5 auth-password private123 priv  DES priv-password
public123
```

The following example configures configure encrypted passwords.

```
device# configure terminal
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# configure terminal
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** }]

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** { **vrf-name** }]

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.

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.

Examples

The following example creates an entry for SNMPv3 trap IPv4 host 10.23.23.45 associated with SNMP user "snmpadmin1."

```
device# configure terminal
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# configure terminal
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# configure terminal
device(config)# snmp-server v3host 10.24.61.10 public use-vrf default-vrf
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** }

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# configure terminal
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# configure terminal
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# configure terminal
device(config)# no snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
!
```

History

Release version	Command history
18s.1.01	This command was introduced.

source

Configures the monitoring session.

Syntax

source [**ethernet** *slot/port* | **destination** | **direction** [**rx** | **tx** | **both**]

no source [**ethernet** *slot/port* | **destination** | **direction** [**rx** | **tx** | **both**]

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.

destination

Use this parameter to specify the interface.

direction rx

Specifies to monitor the receiving traffic.

direction tx

Specifies to monitor the transmitting traffic

direction both

Specifies to monitor transmitting and receiving traffic.

Modes

Monitor session configuration mode

Usage Guidelines

Enter **no source** followed by the identifying parameters to delete the port mirroring connection for the specified interface.

Examples

To enable session 22 for monitoring traffic:

```
device# configure terminal
device(config)# monitor session 22
device(config-session-22)# source ethernet 0/1 destination ethernet 0/15 direction both
```

History

Release version	Command history
17s.1.00	This command was introduced.

source-ip

Configures the source IPv4 address of Precision Time Protocol (PTP) packets.

Syntax

source-ip *IP-address*

no source-ip

Command Default

See Parameters.

Parameters

ip-address

Source IPv4 address of PTP packets. The default is 0.0.0.0.

Modes

PTP configuration mode

Usage Guidelines

This command configures the source IPv4 address for all PTP packets, and is switch specific. The IPv4 address is required to support unicast communication between master and slave clocks.

Only IPv4 addresses, without masks, are allowed.

Use the **no** form of this command to revert to the default source IPv4 address.

Examples

To configure a nondefault source IPv4 address:

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# source-ip 10.1.1.1
```

To revert to the default source IPv4 address (0.0.0.0):

```
device# configure terminal
device(config)# protocol ptp
device(config-ptp)# no source-ip
```

History

Release version	Command history
17s.1.00	This command was introduced.

span session

Configures the SPAN session.

Syntax

span session *session_id*

no span session *session_id*

Parameters

session_id

Designates the session number for the flow-based SPAN session.

Modes

Policy class configuration mode

Usage Guidelines

Use the **no span session** *session-id* command to delete the session.

Examples

The following example configures a SPAN session.

```
device(config)# policy-map myPolicyMap
device(config-policymap)# class myClass
device(config-policymap-class)# span session 1
```

History

Release version	Command history
17s.1.01	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree autoedge
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
: Brocade Control Mac

Modes

Interface configuration mode

Usage Guidelines

This command will only take effect when the protocol is PVST+ or R-PVST+.

The PVST+ and R-PVST+ protocols are supported. The PVST and R-PVST protocols—proprietary to Cisco—are not supported.

Enter **no spanning-tree bpdu-mac 0100.0ccc.cccd** to remove the address.

Examples

The following example sets the MAC address of the BPDU.

```
device# configure terminal
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree cost 128
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree edgeport
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# spanning-tree edgeport
device(conf-if-eth-0/5)# spanning-tree edgeport bpdu-guard
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree guard root
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

Rapid transition is enabled for STP.

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 0/5
device(conf-if-eth-0/5)# spanning-tree link-type shared
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree portfast
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# spanning-tree portfast
device(conf-if-eth-0/5)# spanning-tree portfast bpdu-guard
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree priority 16
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree restricted-role
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/5
device(conf-if-eth-0/5)# spanning-tree restricted-tcn
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/1
device(conf-if-eth-0/1)# spanning-tree shutdown
```

To disable spanning tree on a specific interface:

```
device# configure terminal
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# spanning-tree shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

speed (Ethernet)

Sets the speed negotiation value on an Ethernet interface.

Syntax

SLX 9140 (ports 1-48): **speed** { **1000** | **10000** | **25000** | **auto**}

SLX 9140 (ports 49-54): **speed** { **40000** | **100000** | **auto**}

SLX 9240 (ports 1-32): **speed** { **40000** | **100000** | **auto**}

Command Default

The default speed of the port.

SLX 9140: 10Gbps is the default speed of the first 48 ports. For the last 6 ports, the default speed is 100Gbps.

SLX 9240: 100 Gbps is the default speed.

Parameters

1000
Forces the speed to 1 Gbps.

10000
Forces the speed to 10 Gbps.

25000
Forces the speed to 25 Gbps.

40000
Forces the speed to 40Gbps.

100000
Forces the speed to 100 Gbps.

auto
Allows the interface to configured the speed based on the detected optic type.

Modes

Interface subtype configuration mode

Usage Guidelines

SLX 9140 port management includes the following:

- Supports 54 ports in total. The first 48 ports support 10G and 25G speed (default is10G). Breakout is not supported.
- The last 6 ports support 40G and 100G (default 100G) and breakout is supported.
- Forward Error Correction (FEC) is supported for 25G and 100G speed.

SLX 9240 port management includes the following:

- Supports 32 ports in total. All ports support 40G and 100G (default 100G) and breakout is supported.
- FEC is supported for 100G speed.

Examples

The following example changes the speed to 100G.

```
device# configure terminal
device(config)# interface Ethernet 0/10
device(conf-if-eth-0/10)# speed 100000
```

History

Release version	Command history
17s.1.00	This command was introduced.

speed (LAG)

Sets the allowed speed of member links that can be added in the LAG. Member links with speed other than the configured value will be administratively shut down.

Syntax

speed { **1000** | **10000** | **25000** | **40000** | **100000** }

Command Default

Speed is 100000

Parameters

1000
Forces the speed to 1 Gbps.

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.

Modes

Port-channel interface configuration mode

Usage Guidelines

Configuring member ports with different speed under a LAG is allowed. However, the interfaces that come up with non-matching port speed are brought down with speed mismatch exception.

Examples

The following example sets the speed on the LAG interface as 10 Gbps.

```
device# configure terminal
device(config)# interface port-channel 30
device(conf-Port-channel-30)# speed 10000
```

History

Release version	Command history
17s.1.00	This command was introduced.

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; if no encryption algorithm is specified, the default (**3des**) is used. Supported algorithms include the following:

3des

Triple Data Encryption Standard (DES). This is the default setting.

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 v valid value is 0.

management
Specifies a management interface.

ve *vlan-id*
Range is from 1 through 4096.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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, in a non-cbc or comma separated list of supported cipher algorithms such as 3des-cbc,aes192-cbc,aes128-ctr,aes192-ctr, and so on.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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-cbcr

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 diffie-hellman-group14-sha1

no ssh client key-exchange

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, 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 client key-exchange to DH Group 14:

```
device# configure terminal
device(config)# ssh client key-exchange diffie-hellman-group14-sha1
```

To restore the ssh client key-exchange to default value:

```
device# configure terminal
device(config)# no ssh client key-exchange
```

History

Release version	Command history
17s.1.00	This command was introduced.

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-md5, hmac-sha1, hmac-sha2-256, and hmac-sha2-512. 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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, in a non-cbc or comma separated list of supported cipher algorithms such as 3des-cbc,aes192-cbc,aes128-ctr,aes192-ctr, and so on.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

ssh server cipher non-cbc

Sets the SSH server's cipher list to non-cbc ciphers for the SSH server.

Syntax

ssh server cipher non-cbc

no ssh server cipher non-cbc

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh server cipher non-cbc** command remove the non-cbc cipher list from the ssh client.

Examples

Sets the SSH server's cipher list to non-cbc ciphers.

```
device# configure terminal
device(config)# ssh server cipher non-cbc
device(config)# do show running-config ssh
ssh server non-cbc
ssh client non-cbc
```

History

Release version	Command history
17s.1.00	This command was introduced.

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**] | **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**]

Generates the RSA key, in either the 1024 or 2048 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.

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

This example generates a DSA key:

```
device# configure terminal
device(config)# ssh server key dsa
```

This example generates an RSA 1024 bit key:

```
device# configure terminal
device(config)# ssh server key rsa 1024
```

This example generates an ECDSA 256 bit key:

```
device(config)# ssh server key ecdsa 256
```

This example removes the DSA key:

```
device(config)# no ssh server key dsa
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 diffie-hellman-group14-sha1

no ssh server key-exchange

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# configure terminal
device(config)# ssh server key-exchange diffie-hellman-group14-sha1
```

To restore the SSH server key-exchange to default value:

```
device# configure terminal
device(config)# no ssh server key-exchange
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 default MAC required. Your choices are hmac-md5, hmac-sha1, hmac-sha2-256, and hmac-sha2-512. 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 reset the rekey-interval to the default value.

Examples

To set the SSH server rekey interval to 1200 seconds:

```
device# configure terminal
device(config)# ssh server rekey-interval 1200
```

To restore the SSH server rekey interval to the default value:

```
device# configure terminal
device(config)# no ssh server rekey-interval
```

History

Release version	Command history
17s.1.00	This command was introduced.

ssh server shutdown

Disables 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

Enter **no ssh server shutdown** to enable SSH service.

The use of the **use-vrf** keyword brings down the server only for the specified VRF. The user can shut down any server in any VRF, including the management and default VRF.

When this command is executed and a VRF is not specified by means of the **use-vrf** keyword, the server is brought down only in the management VRF ("mgmt-vrf") (the default VRF for this command).

Examples

To shut down SSH service on the management VRF:

```
device# configure terminal
device(config)# ssh server shutdown
```

To shut down SSH service for a user-defined VRF:

```
device# configure terminal
device(config)# ssh server use-vrf myvrf shutdown
```

To enable SSH service on the management VRF:

```
device# configure terminal
device(config)# no ssh server shutdown
```

To enable SSH service:

```
device# configure terminal
device(config)# no ssh server shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

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#
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified. Inside the Linux shell—by default—an SLX-OS user no longer has root access, but rather limited access.

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.

The **no** form of the command restores the defaults.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

statistics (bridge domain)

Enables ingress and egress statistics on a bridge domain.

Syntax

statistics

no statistics

Parameters

None

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

statistics (VLAN)

Enables statistics on a VLAN.

Syntax

statistics

no statistics

Command Default

Statistics are disabled.

Parameters

None

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
```

History

Release version	Command history
17s.1.01	This command was introduced.

statistics-enable

Enables statistics for a policy-based forwarding (PBF) destination

Syntax

statistics-enable

Command Default

Statistics are not maintained for the PBF destination.

Modes

PBF-destination configuration mode

Usage Guidelines

The use-case for this command is under Network Packet Broker (NPB) system-mode.

The software limits the number of statistics-enabled PBF destinations per NPB-grid to 2000.

The **no** form of this command disables PBF statistics.

Examples

The following example enables statistics for a PBF destination.

```
device# configure terminal
device(config)# pbf destination 20
device(config-destination-20)# statistics-enable
```

History

Release version	Command history
18s.1.02	This command was introduced.

storm-control ingress

Limits ingress traffic on a specified interface.

Syntax

storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** } { **limit-bps** | **limit-percent** } *rate* [{ **monitor** | **shutdown**] }

no storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** } { **limit-bps** | **limit-percent** } *rate* [{ **monitor** | **shutdown**] }

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.

limit-percent
Specifies that the value given to the *rate* parameter is in percentage of capacity of the interface. If the traffic on the interface reaches this percentage of capacity, 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.

- Range if you are specifying rate in bps: 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.
- Range if you are specifying rate in percent of interface capacity: 0 to 100.

monitor
Specifies that, if a rate limit is reached within a five-second sampling period, a log message gets sent. A log message is generated upon the first occurrence of such an event. Subsequent log messages are generated only at the end of one complete sample interval in which no rate limits are reached.

shutdown
Specifies that, if a rate limit is exceeded within a five-second sampling period, the interface will be shut down. You must manually re-enable the interface after a shutdown.

Modes

Interface configuration mode

Usage Guidelines

This command limits the amount of broadcast, unknown unicast, and multicast (BUM) ingress traffic on a specified interface. The *shutdown* parameter monitors the status of the configured rate limit every five seconds, and if the maximum defined rate is exceeded the corresponding interface is shut down until you re-enable it using the **no shut** command.

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

To configure storm control on an Ethernet interface, with a rate limited to 1000000 bps:

```
device(config)# interface ethernet 0/3
device(conf-if-eth-0/3)# storm-control ingress broadcast 1000000
```

History

Release version	Command history
17s.1.00	This command was introduced.

strip-802-1br

Removes 802.1BR headers from incoming packets, for forwarding to the next processing port—for further filtering and forwarding.

Syntax

strip-802-1br

no strip-802-1br

Command Default

802.1BR header stripping is disabled.

Modes

Ethernet interface configuration mode

Usage Guidelines

This feature applies to both IPv4 and IPv6 traffic.

Enabling 802.1BR header-stripping on an interface requires the following settings:

- NPB system mode:

```
device# configure terminal
device(config)# hardware
device(config-hardware)# system-mode ?
Possible completions:
  [default]
  default   default mode
  npb       Network Packet Broker mode
device(config-hardware)# system-mode npb
```

- The default header-mode—802.1BR—must be enabled. If VN-Tag header-mode is enabled, restore 802.1BR mode:

```
device(config)# interface Ethernet 0/2
device(config-if-eth-0/2)# no allow-vn-tag
```

- Enable 802.1BR header stripping on the interface:

```
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# strip-802-1br
```

If a tunneled frame has an 802.1BR tag in the outer L2 header, VXLAN, NVGRE, ERSPAN, or L2-over-MPLS/pseudo-wire header-stripping also deletes the 802.1BR tag. (802.1BR tags in the inner L2 header are not supported.)

If both MPLS and 802.1BR header-stripping are configured, MPLS is always implemented. However, details vary between IP-over-MPLS and L2-over-MPLS regarding 802.1BR tags:

- Under IP-over-MPLS, only the MPLS labels are stripped; 802.1BR tags are not affected. The header diagram for this case is as follows:

IP-over-MPLS frame headers			
L2 (802.1BR tag)	MPLS	IPv4	TCP

- Under L2-over-MPLS (pseudo-wire), both the outer L2 (with 802.1BR tag) and the MPLS header are stripped. The header diagram for this case is as follows:

IP-over-MPLS frame (pseudo-wire) headers				
L2 (802.1BR tag)	MPLS	L2	IPv4	TCP

If interfaces with header-stripping enabled are included in a port-channel, the header stripping remains enabled, but only for traffic entering those interfaces.

The **no** form of this command disables 802.1BR header-stripping on the interface.

Examples

The following example enables 802.1BR header-stripping on the interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# strip-802-1br
```

The following example disables 802.1BR header-stripping on the interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# no strip-802-1br
```

History

Release version	Command history
18s.1.00	This command was introduced.

strip-vn-tag

Removes Virtual NIC (VN)-tag headers from incoming packets, for forwarding to the next processing port—for further filtering and forwarding.

Syntax

strip-vn-tag

no strip-vn-tag

Command Default

VN-tag header stripping is disabled.

Modes

Ethernet interface configuration mode

Usage Guidelines

This feature applies to both IPv4 and IPv6 traffic.

Enabling VN-Tag header-stripping on an interface requires the following settings:

- NPB system mode. For example:

```
device# configure terminal
device(config)# hardware
device(config-hardware)# system-mode ?
Possible completions:
  [default]
  default   default mode
  npb       Network Packet Broker mode
device(config-hardware)# system-mode npb
```

- VN-Tag header-mode must be enabled. If 802.1BR mode:

```
device(config)# interface Ethernet 0/2
device(config-if-eth-0/2)# no allow-vn-tag
```

If a tunneled frame has a VN-Tag in the outer L2 header, VXLAN, NVGRE, ERSPAN, or L2-over-MPLS/pseudo-wire header-stripping also deletes the VN-Tag. (VN-Tags in the inner L2 header are not supported.)

If both MPLS and VN-Tag header-stripping are configured, MPLS is always implemented. However, details vary between IP-over-MPLS and L2-over-MPLS regarding VN-Tags:

- Under IP-over-MPLS, only the MPLS labels are stripped; VN-Tags are not affected. The header diagram for this case is as follows:

IP-over-MPLS frame headers			
L2 (VN-Tag)	MPLS	IPv4	TCP

- Under L2-over-MPLS (pseudo-wire), both the outer L2 (with VN-Tag) and the MPLS header are stripped. The header diagram for this case is as follows:

IP-over-MPLS frame (pseudo-wire) headers				
L2 (VN-Tag)	MPLS	L2	IPv4	TCP

If interfaces with header-stripping enabled are included in a port-channel, the header stripping remains enabled, but only for traffic entering those interfaces.

The **no** form of this command disables VN-tag header-stripping on the interface.

Examples

The following example enables VN-tag header-stripping on the interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# strip-vn-tag
```

History

Release version	Command history
18s.1.00	This command was introduced.

strip-vxlan

Removes Virtual Extensible LAN (VXLAN) headers from incoming packets, for forwarding to the next processing port—for further filtering and forwarding.

Syntax

strip-vxlan

no strip-vxlan

Command Default

VXLAN header-stripping is disabled.

Modes

Ethernet interface configuration mode

Usage Guidelines

This feature is relevant only under NPB system mode.

On an interface, you can enable both VXLAN and NVGRE header-stripping. (VXLAN and NVGRE are mutually exclusive flows.)

This feature applies to both IPv4 and IPv6 traffic.

The final Frame Check Sequence (FCS) is updated with a recalculated CRC.

If interfaces with header-stripping enabled are included in a port-channel, the header stripping remains enabled, but only for traffic entering those interfaces.

For tunneled frames, header-stripping affects only the outer, encapsulation headers. For example:

- If both ERSPAN and VXLAN header-stripping are configured on the ingress interface, only the ERSPAN headers are stripped. The header diagram for this case is as follows:

ERSPAN headers				VXLAN headers				Payload frame headers		
L2	IPv4	GRE	ERSPAN	L2	iIPv4	UPD	VXLAN	L2	IPv4	TCP

- If both VXLAN and MPLS header-stripping are configured, only VXLAN headers are stripped. The header diagram for this case is as follows:

VXLAN headers				Payload frame headers			
L2	IPv4	UDP	VXLAN	L2	MPLS	IPv4	TCP

The **no** form of this command disables VXLAN header-stripping on the interface.

Examples

The following example enables VXLAN header-stripping on the interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# strip-vxlan
```

History

Release version	Command history
18s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

You can configure up to 4 address ranges.

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.

The **no** form of the command disables route summarization.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

switch-attributes

Configures the chassis or host name for the device.

Syntax

switch-attributes { **chassis-name** *chassis-name* } | { **host-name** *host-name* }

no switch-attributes { **chassis-name** | **host-name** }

Command Default

The default chassis name is SLX9140-0.

The default host name is SLX.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/9
switch(conf-if-eth-0/9)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

switchport access

Specifies the VLAN for Layer 2 switchport access mode.

Syntax

switchport access { **vlan** *vlan_id* }

no switchport access { **vlan** }

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 1 through 4090.

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
device(config)# interface ethernet 0/9
device(conf-if-eth-0/9)# switchport access vlan 100
```

To set the PVID to the default VLAN 1 on a specific port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 44
device(config-Port-channel-44)# no switchport access vlan
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 0/9
switch(conf-if-eth-0/9)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 subtype configuration mode

Usage Guidelines

By assigning this mode, the user can configure an untagged logical interface on the specified port. Any ingress tagged or untagged packet is discarded until a switchport classification or native VLAN classification is configured. To disable this functionality, simply 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

Configure a trunk port without a default native VLAN, then explicitly configure the native VLAN.

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-0/1)# switchport mode trunk-no-default-native
switch(config-if-eth-0/1)# switchport trunk tagged
```

History

Release version	Command history
17s.1.00	Added usage guideline limitation.
17s.1.00	This command was introduced.

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# configure terminal
device(config)# interface Ethernet 0/2
device(conf-if-eth-0/2)# switchport
device(conf-if-eth-0/2)# switchport port-security
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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 or 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# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# switchport
device(conf-if-eth-0/1)# switchport port-security mac-address 0000.00eb.2d14 vlan 2
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*

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.

Examples

The following example configures the maximum number of MAC addresses used for port MAC security on an interface port as 10:

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# switchport
device(conf-if-eth-0/1)# switchport port-security max 10
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.

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# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# switchport
device(conf-if-eth-0/1)# switchport port-security shutdown-time 4
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*]

Command Default

Sticky MAC learning on the port is not enabled.

Parameters

mac-address *address*
Specifies the MAC address.

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.

Sticky MAC addresses persist even if the port goes down; or if the device reboots, provided the config is saved.

Examples

The following example enables sticky MAC learning on the port and configures port security with sticky MAC address:

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# switchport
device(conf-if-eth-0/1)# switchport port-security sticky
device(conf-if-eth-0/1)# switchport port-security sticky mac-address 0000.0018.747C vlan 5
```

History

Release version	Command history
17s.1.00	This command was introduced.

switchport port-security violation

Configures the violation response action for port security on an interface.

Syntax

switchport port-security violation { **restrict** | **shutdown** }

Command Default

The port shuts downs if port security violation occurs.

Parameters

restrict

Drops the packets that have unknown source addresses until you remove a sufficient number of secure MAC addresses to keep the count within the maximum MAC limit allowed on the interface.

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# configure terminal
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# switchport
device(conf-if-eth-0/1)# switchport port-security violation shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

switchport trunk allowed

Adds or removes VLANs on a Layer 2 interface in trunk mode.

Syntax

switchport trunk allowed { **vlan** | **rspan-vlan** } { **add** *vlan_id* { **ctag** { *id* | *ctag* **-** *range* } | **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, an RSPAN VLAN, or a transport 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.

ctag
Specifies an incoming C-TAG or range of C-TAGs for classified or transport VLANs.

id
C-TAG ID.

range
Range of C-TAG IDs, for example, 100-200, or 10,20,100-200, applicable only if the VLAN is a transport VLAN.

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.

rspan-vlan *vlan_id*
Selects a VLAN for Remote Switched Port Analyzer (RSPAN) traffic monitoring.

remove *vlan_id*
Removes a VLAN that transmits and receives through the Layer 2 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

A transport VF C-TAG can be any VLAN ID that is not used in other classifications or as a 802.1Q VLAN.

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
```

Configure a classified VLAN with a C-TAG:

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 5000 ctag 100
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 6000 ctag 200
```

An 802.1Q vlan specified as a user VLAN cannot be used as a C-TAG in a classified VLAN. The following show conflicts.

- Edge C-TAG 100 is already assigned to VLAN 5000 at the same port:

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 8000 ctag 100
switch(config-if-eth-0/1)# %Error: C-tag is already used.
```

- Edge VLAN 888 was already used in 802.1Q configuration.

```
device# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if-eth-0/1)# switchport trunk allowed vlan add 8000 ctag 888
switch(config-if-eth-0/1)# %Error: Ctag is configured in the allowed range on this port.
```

History

Release version	Command history
17s.1.00	This command was introduced.

switchport trunk default-vlan

Configures tagged or untagged data traffic that does not match any classification rule on a trunk port, supporting service or transport VFs.

Syntax

switchport trunk default-vlan *vlan_id*

no switchport trunk default-vlan *vlan_id*

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

Enter **no switchport trunk default-vlan** *vlan_id* to remove the default VLAN configuration.

Examples

Classify all nonmatching traffic except native VLAN traffic to the transparent default VLAN:

```
device(config-if-eth-0/1)# switchport trunk default-vlan 6000
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 $1/(2^{\log \text{seconds}})$.

Configuring this interval on an edge port overrides the switch (global) default.

ATTENTION
Do not configure a rate slower than the default on links between SLX-OSdevices.

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

Examples

The following example configures 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
```

The following example reverts 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

sysmon sfm-walk

Enables SFM walk.

Syntax

sysmon sfm-walk [**start** | **stop**]

Parameters

start

Enable SFM walk.

stop

Disables SFM walk.

Modes

Privileged EXEC mode

Usage Guidelines

By default, SFM walk is disabled.

Examples

```
device# sysmon sfm-walk start
```

History

Release version	Command history
17s.1.00	This command was introduced.

system packet-timestamp egress

Configures how a timestamp is processed when the packet is forwarded on the egress interface.

Syntax

system packet-timestamp egress { **add** | **remove** | **replace** }

no system packet-timestamp egress

Command Default

No processing is applied on the egress interface.

Parameters

add

Specifies that the time the packet ingresses the switch is appended to the end of the payload on the egress interface. The timestamp is used to recalculate the frame check sequence (FCS) and is in 8-byte nanosecond format. See the Usage Guidelines.

remove

Specifies that the timestamp in the ingress payload is removed on the egress interface.

replace

Specifies that the timestamp in the ingress payload is replaced by the timestamp on the egress interface.

Modes

Interface subtype configuration mode

Usage Guidelines

ATTENTION
The presence of the timestamp in the ingress payload is effectively indicated by the **system packet-timestamp ingress valid** command. Hardware does not verify whether or not the timestamp is actually in the payload. If the use of the above command specifies that the timestamp be present but the timestamp does not actually exist, hardware overwrites or removes the last eight bytes of payload data.

This command is not allowed on interfaces that are part of a port-channel.

Use the **no** form of this command to disable the processing of packets on the egress interface.

Examples

To specify that the timestamp indicating when the packet ingresses the switch is appended to the end of the payload on an egress port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# system packet-timestamp egress add
```

To specify that the timestamp indicating when the packet ingresses the switch is removed from the end of the payload on an egress port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# system packet-timestamp egress remove
```

To specify that the timestamp indicating when the packet ingresses the switch is replaced by the timestamp on an egress port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# system packet-timestamp egress replace
```

To disable the processing of packets on an egress port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# no system packet-timestamp egress
```

History

Release version	Command history
17s.1.00	This command was introduced.

system packet-timestamp ingress valid

Informs the SLX device whether or not an ingress packet has a timestamp appended to the payload.

Syntax

system packet-timestamp ingress valid

no system packet-timestamp ingress

Command Default

By default, a timestamp is not appended.

Modes

Interface subtype configuration mode

Usage Guidelines

This is supported only on Layer 2 interfaces (nonswitch, switchport, port-channel).

> ATTENTION
> The presence of the timestamp in the ingress payload is effectively indicated by this command. Hardware does not verify whether or not the timestamp is actually in the payload. If the use of this command specifies that the timestamp is appended but the timestamp does not actually exist, then the hardware overwrites or removes the last eight bytes of payload data.

Use the **no** form of this command to inform the SLX device that ingressing frames do not have appended timestamps.

Use the **system packet-timestamp egress** command to configure how the timestamp is processed at the egress interface.

Examples

To specify that a timestamp exists in all payloads that ingress a port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# system packet-timestamp ingress valid
```

To specify that a timestamp does not exist in any payload that ingresses the interface:

```
device# configure terminal
device(config)# interface port-channel 1
device(config-Port-channel-1)# no system packet-timestamp ingress
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example sets the global system description specific to LLDP.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# system-description SLXS
```

History

Release version	Command history
17s.1.00	This command was introduced.

system-mode

Sets the system mode.

Syntax

system-mode { **default** | **npb** }

Parameters

default

Specifies the default system mode.

npb

Specifies the Network Packet Broker (NPB) system mode.

Modes

Hardware configuration mode

Usage Guidelines

In NPB mode, Layer 2 and Layer 3 forwarding, protocols, and services such as SPAN and SFLOW are not supported. Extreme recommends not to use any of these configurations in NPB mode. If these features are required, use default mode.

Examples

The following example indicates that the current mode is default. The value displayed within brackets ([ ]) is the current mode.

NOTE

The **show running-config hardware** command also displays the current mode.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# system-mode ?
Possible completions:
  [default]
  default   default mode
  npb       Network Packet Broker mode
```

The following example sets the NPB system mode and reloads the system.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# system-mode npb
%Warning: To activate the new system-mode config, please reboot the system using 'reload system'.
device(config-hardware)# exit
device(config)# exit
device# reload system
Warning: This operation will cause the chassis to reboot and requires all existing telnet, secure
telnet and SSH sessions to be restarted.
Unsaved configuration will be lost. Please run `copy running-config startup-config` to save the current
configuration if not done already.
Are you sure you want to reboot the chassis [y/n]? y <Enter>
```

The following example resets the default system mode.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# system-mode default
%Warning: To activate the new system-mode config, please reboot the system using 'reload system'.
```

History

Release version	Command history
17s.1.00	This command was introduced.

system-monitor

Manages the monitoring of FRUs and sets a variety of alerts when thresholds are exceeded.

Syntax

system-monitor { **LineCard** [**alert** [**action** [**all** | **email** | **none** | **raslog**]] | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]]] | **cid-card** [**alert** [**action** | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]] | **compact-flash** [**threshold** [**down-threshold** | **marginal-threshold**]] | **fan** [**alert** [**action** | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]] | **power** [**alert** [**action** | **state** [**all** | **faulty** | **inserted** | **none** | **on** | **removed**]] | **threshold** [**down-threshold** | **marginal-threshold**]] **sfp** [**alert** [**action state**]] **temp** [**threshold** [**down-threshold** | **marginal-threshold**]] }

no system-monitor

Command Default

For system monitoring defaults, see the "System Monitor" chapter in the *Extreme SLX-OS Monitoring Configuration Guide* .

Parameters

LineCard
Specifies alerts and thresholds for line cards.

cid-card
Specifies alerts and thresholds for the chassis ID card.

compact-flash
Specifies thresholds for the compact flash device.

fan
Specifies alerts and thresholds for the fans.

power
Specifies alerts and thresholds for the power supplys.

sfp
Specifies alerts for the small form-factor pluggable devices.

temp
Specifies thresholds for the temperature sensors.

alert
Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

action
Specifies the response type.

all
Specifies that e-mail and RASLog messaging are used.

email
Specifies that an e-mail message is sent.

none
Specifies that no message is sent.

raslog
Specifies RASLog messaging.

state
Specifies the hardware state to be monitored.

all
Specifies that all hardware states are monitored.

faulty
Specifies that hardware is monitored for faults.

inserted
Specifies that the insertion state of hardware is monitored.

none
Specifies that no hardware states are monitored.

on
Specifies that the hardware on/off state is monitored.

removed
Specifies that the removal of hardware is monitored.

threshold
Specifies the monitoring of thresholds

down-threshold
Specifies an integer value that, when exceeded, indicates when hardware is down.

marginal-threshold
Specifies an integer value that, when exceeded, indicates when hardware is operating marginally.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure field-replaceable unit (FRU) monitoring and actions. Depending on these configuration settings, a variety of actions are generated when there is a change in FRU state.

Examples

Typical command example that sets the

```
device# configure terminal
device(config)# system-monitor sfm threshold down-threshold 3 marginal-threshold 2
device(config)# system-monitor cid-card alert state faultyinserted action email
```

History

Release version	Command history
17s.1.00	This command was introduced.

system-monitor-mail

Configures Fabric Watch e-mail alerts on the device.

Syntax

system-monitor-mail { **fru** | **interface** | **relay** { *host_ip* | *domain_name* } | **security** | **sfp** } **enable** | *email-id*]

no system-monitor-mail

Command Default

The default source is disabled.

Parameters

fru
Configures e-mail alerts for FRUs.

interface
Configures e-mail alerts for interfaces.

relay
Configures the relay host for e-mail to work in a non-DNS environment.

host_ip
Specifies the IPv4 address of the mail server.

domain_name
Specifies the domain that corresponds to the e-mail ID.

security
Configures e-mail alerts for security.

sfp
Configures e-mail alerts for SFPs.

enable
Enables or disables e-mail alerts for the above options.

email-id
Specifies the e-mail address to where the alert will be sent.

Modes

Global configuration mode

Usage Guidelines

For an e-mail alert to function correctly, add the IP addresses and host names to DNS in addition to configuring the domain name and name servers. Both relay parameters (the host IP address and the domain name) must be configured in a non-DNS environment. In a DNS environment, only the host IP address is required).

Examples

The following example creates a mapping.

```
device# configure terminal
device(config)# system-monitor-mail relay host-ip 1.2.3.4 domain-name abc.example.com
```

The following example deletes the mapping.

```
device# configure terminal
device(config)# no system-monitor-mail relay host-ip 1.2.3.4
```

The following example changes the domain name.

```
device# configure terminal
device(config)# system-monitor-mail relay host-ip 1.2.3.4 domain-name mail.example.com
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

The following example specifies a system name for the LLDP.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# system-name LLDP_01
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*

Parameters

string

Specifies a route map to be whose attributes are to be preserved. Valid values range 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 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.

The **no** form of the command removes the table map.

Examples

The following 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
```

The following 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
```

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

tacacs-server

Configures a Terminal Access Controller Access-Control System plus (TACACS+) server.

Syntax

tacacs-server { **host** *hostname* [**use-vrf** *vrf-name*]

tacacs-server { **source-ip** [*chassis-ip*] }

[**port** *portnum*]

[**protocol** { **chap** | **pap** }]

[**key** *shared_secret*]

[**encryption-level** *value_level*]

[**timeout** *secs*]

[**retries** *num*]

no tacacs-server { **host** *hostname* | **source-ip** [*chassis-ip*] } [**use-vrf** *vrf-name*]

Parameters

host hostname
Specifies the IP address or domain name of the TACACS+ server. IPv4 and IPv6 addresses are supported.

use-vrf *vrf-name*
Specifies a VRF though which to communicate with the TACACS+ server. See the Usage Guidelines.

tacacs-server source-ip [**chassis-ip**]
Specifies the chassis IP address as the source IP address for TACACS+ authentication and accounting.

port *portnum*
Specifies the authentication port. 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 8 and 40 characters in length. The default key is **sharedsecret** . The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and 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 (such as 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.

Executing the **no** form of the **tacacs-server** command attributes resets the specified attributes to their default values.

NOTE

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 throw an error that requests this value be set to **0**.

Before downgrading to a version that doesn't support **tacacs-server source-ip**, you must remove the source-ip configuration using **no tacacs-server source-ip**. Otherwise, the firmware download process throws 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").

Examples

To configure 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)#
```

To modify an existing 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"
```

To delete a TACACS+ server:

```
device# configure terminal
device(config)# no tacacs-server host 10.24.65.6
```

To configure 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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.03	This command was enhanced for the **use-vrf** and **encoding** commands.

telemetry profile

Enters telemetry-profile configuration mode for a telemetry profile.

Syntax

telemetry profile enhanced-queue-discard-pkts default_enhanced_queue_discard_pkts_statistics

telemetry profile event default_event_statistics

telemetry profile interface default_interface_statistics

telemetry profile lldp default_lldp_statistics

telemetry profile pbr default_pbr_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

Accesses configuration mode for profile **default_enhanced_queue_discard_pkts_statistics** of the **enhanced-queue-discard-pkts** profile type—for tracking discarded-packet statistics.

event default_event_statistics

Accesses configuration mode for profile **default_event_statistics** of the **event** profile type—for tracking up/down interface events

interface default_interface_statistics

Accesses configuration mode for profile **default_interface_statistics** of the **interface** profile type—for tracking interface statistics.

lldp default_lldp_statistics

Accesses configuration mode for profile **default_lldp_statistics** of the **lldp** profile type—for tracking LLDP neighbor information, including link states.

pbr default_pbr_statistics

Accesses configuration mode for profile **default_pbr_statistics** of the **pbr** profile type—for tracking policy-based routing (PBR) statistics.

queue default_queue_statistics

Accesses configuration mode for profile **default_queue_statistics** of the **queue** profile type—for tracking queue statistics.

system-utilization default_system_utilization_statistics

Accesses configuration mode for profile **default_system_utilization_statistics** of the **system-utilization** profile type—for tracking system utilization statistics.

Modes

Global configuration mode

Usage Guidelines

The **no** option is not supported for this command.

If a telemetry profile has no attributes, no information is streamed to the collector.

The statistics gathered by the default_enhanced_queue_discard_pkts_statistics profile are:

- Interval
- ethernet interfaces
- Discard packets

The statistics gathered by the default_event_statistics profile are:

- Event class
- Severity
- Payload
- Timestamp

The statistics gathered by the default_interface_statistics profile are:

- ethernet and port-channel interfaces
- interval
- In/Out packets
- In/Out unicast packets
- In/Out broadcast packets
- In/Out multicast packets
- In/Out packets per second
- In/Out bandwidth
- In/Out link-utilization
- In/Out octets
- In/Out errors
- In/Out CRC errors
- In/Out discards

The statistics gathered by the default_lldp_statistics profile are:

- interval
- Ethernet interface
- if-name
- update-type
- local-port
- local-chassis-id
- remote-port
- remote-chassis-id

- speed
- local-lag-id
- remote-lag-id
- link-state

The statistics gathered by the default_pbr_statistics profile are:

- ethernet and port-channel interfaces
- interval
- acl-byte-count
- acl-hit-count
- acl-name
- acl-seq-num
- if-name
- num-rules
- route-map

The statistics gathered by the default_queue_statistics profile are:

- interval
- ethernet interfaces
- discard-byte-count
- discard-pkt-count
- enq-byte-count
- enq-pkt-count

The system utilization statistics gathered by the default_system_utilization_statistics profile are:

- Interval
- Total system memory
- Total used memory
- Total free memory
- Cached memory
- Buffers
- Total swap memory
- User free memory
- Kernel free memory
- Total swap memory
- Total free swap memory
- Total used swap memory
- User process
- System process
- Niced process
- In/out wait
- HW interrupt

- SW interrupt
- Idle state
- Steal time
- Up time

Examples

The following example enters telemetry-profile configuration mode for the default_interface_statistics profile.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)#
```

History

Release version	Command history
17s.1.00	This command was introduced.
18s.1.00	Added support for **enhanced-queue-discard-pkts** and **queue** profile types.
18s.1.02	Added support for **event**, **lldp**, and **pbr** profile types.

telemetry server

Enters telemetry-server configuration mode.

Syntax

telemetry server

Command Default

Telemetry-server configuration mode is not active.

Parameters

use-vrf *vrf-name*
(Not supported) Specifies a 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 a 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

telnet server

Configures the Telnet server on the device.

Syntax

telnet server standby enable

telnet server [**use-vrf** *name*] **shutdown**

no telnet server {**standby** | [**use-vrf** *name*] **shutdown**}

Command Default

The Telnet service is enabled by default.

Telnet service on the standby switch is disabled.

Parameters

standby enable
Enables the Telnet server on the standby switch.

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 disable Telnet service on the standby switch, or re-enable the Telnet service on the device. If you include the VRF name, the Telnet server for the VRF is re-enabled.

Shutting down the Telnet service forcibly disconnects all Telnet sessions running on a device.

When you use the **telnet server shutdown** command without a user-defined VRF, the service is shut down on mgmt-vrf only.

Telnet services are associated and started on mgmt-vrf and default-vrf.

Telnet server can be enabled on a maximum number of six VRFs.

Examples

The following example shuts down the Telnet server on the device.

```
device# configure terminal
device(config)# telnet server shutdown
```

History

Release version	Command history
17s.1.00	This command was introduced.

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**.

Use the **no** form of the command to reset the default timeout or disable monitoring.

Use the **terminal no length** command to reset the default number of displayed lines.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

threshold-monitor cpu

Configures monitoring of CPU usage of the system and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor cpu { [**actions** [**loginfo none** | | **raslog** [**limit** *limit_when_reached* | **poll** *polling_interval* | **retry** *number_of_retries*]]}

no threshold-monitor cpu

Parameters

actions
Specifies the action to be taken when a threshold is exceeded.

loginfo
Collects diagnostic data along with RASLOG.

none
No action is taken.

raslog
Specifies RASLog messaging.

limit
Specifies the baseline CPU usage limit as a percentage of available resources.

limit_when_reached
When the limit set by this parameter is exceeded, a RASLog WARNING message is sent. When the usage returns below the limit, a RASLog INFO message is sent. Valid values range from 0 through 80 percent. The default is 70 percent.

poll
Specifies the polling interval in seconds.

polling_interval
The range is from 0 through 3600. The default is 120

retry
Specifies the number of polling retries before desired action is taken.

number_of_retries
Range is from 1 through 100. The default is 3.

Modes

Global configuration mode

Usage Guidelines

This command sends a RASLog WARNING message when configured thresholds are exceeded.

Examples

```
device# configure terminal
device(config)# threshold-monitor cpu actions rasloglimit 50 poll10
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 { **actions** [**none**|**loginfo**|**raslog**] |**high-limit** *percent* | **limit** *percent* | **low-limit** *percent* | **poll** *polling_interval* | **retry** *number_of_retries* }

no threshold-monitor memory

Parameters

actions

Specifies the action to be taken when a threshold is exceeded.

none

No action is taken. This is the default.

loginfo

Collects diagnostic data along with RASLog.

raslog

Specifies RASLog messaging.

high-limit

Specifies an upper limit for memory usage as a percentage of available memory.

percent

This value must be greater than the value set by **limit**. When memory usage exceeds this limit, a RASLog CRITICAL message is sent. Values range from 0 through 80 percent. The default is 70 percent.

limit

Specifies the baseline memory usage limit as a percentage of available resources.

percent

When this value is exceeded, a RASLog WARNING message is sent. When the usage returns below the value set by **limit** , a RASLog INFO message is sent. Values range from 0 through 80 percent. The default is 60 percent.

low-limit

Specifies a lower limit for memory usage as percentage of available memory.

percent

This value must be smaller than the value set by **limit**. When memory usage exceeds or falls below this limit, a RASLog INFO message is sent. The default is 40 percent.

poll

Specifies the polling interval in seconds.

polling_interval

The range is from 0 through 3600. The default is 120

retry

Specifies the number of polling retries before desired action is taken.

number_of_retries
Range is from 1 through 100. The default is 3.

Modes

Global configuration mode

Examples

```
device# configure terminal
device(config)# threshold-monitor memory actions none high-limit 80 low-limit 50 limit 70 retry 2 poll
30
```

History

Release version	Command history
17s.1.00	This command was introduced.

threshold-monitor sfp

Configures monitoring of SFP parameters.

Syntax

threshold-monitor sfp { [**apply** *policy_name* | **pause** | **policy** *policy_name*] **type** *SFP_type* **area** *parameters* **alert** [**above** [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **none** | **raslog**] | **lowthresh-action** [**all** | **email none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **none raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] }

no threshold-monitor sfp

Command Default

By default, SFP is not monitored.

Parameters

apply *policy_name*

Applies a custom policy that has been created by the **policy** operand.

pause

Pause monitoring.

policy

Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.

policy_name

Name of a custom policy configuration that can be saved and applied by means of the **apply** operand.

type

Specifies the SFP type. Possible completions are as follows:

1GLR

— SFP Type 1GLR

1GSR

— SFP Type 1GSR

10GLR

— SFP Type 10GLR

10GSR

— SFP Type 10GSR

10GUSR

— SFP Type 10GUSR

100GSR

— SFP Type 100GSR

QSFP

— SFP type QSFP

area

Specifies one of the following SFP parameters to be monitored. See Defaults, below.

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 µW).

Temperature

Measures the temperature of the SFP, in degrees Celsius.

Voltage

Measures the voltage supplied to the SFP.

alert

Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

above

Enables setting a value for **highthresh-action**, which specifies the action to be taken when a high threshold is exceeded.

below

Enables setting a value for **highthresh-action** and **lowthresh-action**, which specifies the action to be taken when a low threshold is exceeded.

all

Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of **highthresh-action** only.

all

Specifies that email and RASLog messaging are used.

email

Specifies that an email message is sent.

none

Specifies that no alert is sent.

raslog

Specifies RASLog messaging.

limit

Specifies the percent of threshold usage, from 0 through 80. The default is 75.

poll

Specifies the polling interval in seconds, from 0 through 3600. The default is 120.

retry

Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.

threshold

Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.

buffer
An integer value.

high-threshold
An integer value.

low-threshold
An integer value.

timebase
Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.

day
Calculates the difference between a current data value and that value a day ago.

hour
Calculates the difference between a current data value and that value an hour ago.

minute
Calculates the difference between a current data value and that value a minute ago.

none
Compares a data value to a threshold boundary level.

Modes

Global configuration mode

Examples

A typical command might look like this:

```
device# configure terminal
device(config)# threshold-monitor sfp custom type QSFP area rxp threshold high-threshold 2000 low-
threshold 1000
```

History

Release version	Command history
17s.1.00	This command was introduced.

timeout

Specifies 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 default value.

Examples

The following example shows how to configure a wait time (timeout value) 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

timeout (Telemetry)

Defines the timeout value of the LDAP host.

Syntax

timeout { *secs* }

no timeout

Command Default

The timeout is 5 seconds.

Parameters

timeout

Specifies the wait time for a server to respond. The range is 1 through 60 seconds.

Modes

LDAP host configuration mode.

Usage Guidelines

Use the no form of this command to remove the timeout value.

Examples

To add an LDAP server with the timeout set to 8 seconds:

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# timeout 8
```

Executing **no** on an attribute sets it with its default value.

```
device# configure terminal
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# no timeout
```

History

Release version	Command history
17s.1.00	This command was introduced.

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. Valid values range from 0 through 65535 seconds. The default is 60 seconds.

hold-time *holdtime_interval*

Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Valid values range from 0 through 65535 seconds. The default is 180 seconds.

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 configured timers and 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)# 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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* }

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 through 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 through 60000 milliseconds. The default is 0.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 through 60000 milliseconds. The default is 0.

max

Maximum wait time between two consecutive SPF calculations. Valid values range from 0 through 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

timers (OSPFv3)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) timers.

Syntax

timers {**lsa-group-pacing** *interval* | **spf** *start hold* }

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 through 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 through 65535 seconds.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 through 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

tpvm

Provides administrative support for Third-Party Virtual Machine (TPVM) applications.

tpvm auto-boot { **disable** | **enable** }

tpvm disk { **add name** { *disk_name* | **auto** *disk_size* } | **remove name** { *disk_name* | **auto** } }

tpvm help

tpvm install

tpvm password

tpvm start

tpvm stop

tpvm uninstall

Command Default

This feature is not enabled.

Parameters

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.

install
Installs TPVM.

password
Changes the root password on TPVM.

start
Starts TPVM.

stop

Stops TPVM.

uninstall

Uninstalls TPVM if it is already installed.

force

Clears installation or uninstallation errors, then tries to force an uninstallation.

Modes

Privileged EXEC mode

Usage Guidelines

The maximum number of disks is currently 3, and if the number of the allocated disks exceeds it, the **disk add name** subcommand fails. In addition, the total disk capacity is limited to 25 Gbytes. If you exceed this limit when you create a disk, the **disk add name** subcommand fails.

If the **auto** keyword is not used with the **add_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. if the number of allocated disks exceeds this number, the **add_disk** keyword fails.

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..

ATTENTION

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.

The **show ip-address** subcommand requires the qemu-guest-agent package on TPVM. If that package is removed, this subcommand fails.

Examples

To install TPVM if it is not already installed:

```
device# tpvm install
```

To uninstall TPVM if it is installed:

```
device# tpvm uninstall
```

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.

History

Release version	Command history
17s.1.00	This command was introduced.
17s.1.01	This command was modified.
18s.1.01	The show options were moved to **show tpvm**.

traceroute

Traces the network path of packets as they are forwarded to a destination address.

Syntax

traceroute { *IPv4_address* | *host-name* | **ipv6** [*dest-ipv6-address* | *host-name*] } [**interface**] [**maxttl** *value*] [**minttl** *value*] [**src-addr** *src-addr*] [**timeout** *seconds*] [**vrf** *vrf-name*]

Parameters

IPv4_address
Specifies the IPv4 address of the destination device.

host-name
Specifies the hostname of the destination device.

ipv6 *dest-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 *vrf-name*
Name of the VRF. If no VRF is specified, the default-vrf is used.

Modes

Privileged EXEC mode

Usage Guidelines

To use the **traceroute** command on the management VRF, enter **mgmt-vrf**. You must enter the name of the management VRF manually.

Examples

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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-address mask* | *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. The slot number must be 0 if the switch does not contain slots.

port-channel *number*

Specifies the port-channel number. Valid values range from 1 through 6144.

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 0/4 and the track priority to 60:

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 0/6
device(conf-if-eth-0/6)# vrrp-group 1
device(config-vrrp-group-1)# track ethernet 0/4 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

transport

Specifies the transport protocol for gRPC-server telemetry streaming.

Syntax

transport { **tcp** | **ssl** }

no transport { **tcp** | **ssl** }

Command Default

The transport protocol is set to TCP.

Parameters

tcp

Designates TCP for the transport protocol.

ssl

Designates SSL for the transport protocol. SSL provides encryption through TLS.

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.

The **no transport** command resets the transport to TCP.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*]

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.

pattern *posix-ext-regex*
Specifies a POSIX extended regular expression to search within the specified RASlog message ID.

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 0/
[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 0/1 through 0/9.

History

Release version	Command history
17s.1.00	This command was introduced.

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.

Syntax

trigger-function { **OR** | **AND** { **time-window** *seconds* } }

no trigger-function

Command Default

The event-handler action runs if any of the triggers occur (**OR**).

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

tvf-domain

Creates one or more Transparent VLAN Flooding (TVF) domains.

Syntax

tvf-domain *tvf-domain-id*

no tvf-domain *tvf-domain-id*

Parameters

tvf-domain-id

Specifies the ID of the TVF domain. Valid values are from 1 through 4096. To specify a range of domains, insert a hyphen (-) between the beginning and ending integers (for example, 5-16). To specify individual domains and ranges of domains, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas.

Modes

Global configuration mode

Usage Guidelines

This command is available only in NPB system-mode.

TVF forwards packets without CPU intervention—such as MAC learning or MAC destination lookups—enabling line-rate traffic forwarding.

The maximum number of supported TVF domains is 1024.

Under Network Packet Brokering (NPB), TVF domains are required for the traffic replication feature.

The **no** form of this command deletes a specified TVF domain.

Examples

The following example creates a TVF domain.

```
device# configure terminal
device(config)# tvf-domain 10
device(config-tvf-domain-10)# description Sample TVF domain
```

History

Release version	Command history
17s.1.01	This command was introduced.
18s.1.00	The example was modified to include a TVF-domain description.

tvf-domain (interface)

Assigns and removes Transparent VLAN Flooding (TVF) domains from a physical or port-channel interface.

Syntax

tvf-domain { **add** *tvf-domain-id* | **all** | **except** *tvf-domain-id* | **none** | **remove** *tvf-domain-id* }

Command Default

No TVF domains are assigned to the interface.

Parameters

add *tvf-domain-id*

Assigns one or more TVF domains to the interface. 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.

all

Assigns all defined TVF domains to the interface.

except *tvf-domain-id*

Assigns all TVF domains to the interface, except for those specified. 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.

none

Removes all TVF domains assigned to the interface.

remove *tvf-domain-id*

Removes one or more TVF domains from the interface. 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

Interface sub-type configuration mode

Usage Guidelines

Under Network Packet Brokering (NPB), TVF domains are required for the traffic replication feature.

This command is available only in NPB mode.

You can create as many as 4096 TVF domains. Domain members can be tagged and untagged ports. There is no software limitation on the number of member ports.

Examples

The following example assigns a TVF domain that you create to a physical interface.

```
device# configure terminal
device(config)# tvf-domain 10
device(config-tvf-domain-10)# description Sample TVF domain
device(config-tvf-domain-10)# exit
device(config)# interface ethernet 0/30
device(conf-if-eth-0/30)# tvf-domain add 10
device(conf-if-eth-0/30)# no shut
```

History

Release version	Command history
17s.1.01	This command was introduced.

type

Specifies whether a VXLAN overlay gateway uses hardware VXLAN tunnel endpoint (VTEP) or Layer 2 extension integration.

Syntax

type { **layer2-extension** }

Command Default

Layer 2 extension integration is the default behavior.

Parameters

layer2-extension

Specifies Layer 2 extension integration.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

There is no **no** form of this command. The overlay gateway must have a type.

Examples

The following example specifies Layer 2 extension:

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# type layer2-extension
```

History

Release version	Command history
17s.1.01	This command was introduced.

uda access-list

Creates a user-defined ACL (UDA). UDAs offer greater flexibility than other ACLs in defining deny and permit rules. This flexibility is required for certain Network Packet Broker (NPB) scenarios.

Syntax

uda access-list extended *acl-name*

no uda access-list extended *acl-name*

Command Default

No UDA is defined.

Parameters

extended

Specifies an extended ACL. Extended ACLs support source and destination addresses, as well as other parameters. UDAs cannot be standard ACLs, which filter by source address only.

acl-name

Specifies an ACL name unique among all ACLs (Layer 2, Layer 3, and UDAs). 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

Ths command is supported only in NPB system mode.

A UDA starts functioning on an interface—for aggregation, replication, or forwarding—only if the following flow is implemented:

- Create a UDA profile, using the **uda-key profile** command.
- For the profile, specify the header types in the expected packet structure, using the **flow** command.
- For the profile, specify the header fields to match, using the **uda-key** command.
- Apply the profile to the interface, using the **uda-profile-apply** command.
- Create a UDA, using the **uda access-list** command.
- Create one or more permit or deny rules in the UDA, using the [**seq** *seq-value*] { **deny** | **permit** } command.
- Create a route-map, using the **route-map** command.
- Apply the UDA to the route-map, using the **match uda address acl** command.
- In the route-map, specify the egress interface, using the **set interface** or **set next-hop-tvf-domain** command.
- On a physical or port-channel interface, apply the route map to the ingress interface, using the **npb policy route-map** command.

To delete a UDA that is not referenced by any route-map, use the **no** form of this command.

Examples

The following example creates a UDA.

```
device# configure terminal
device(config)# uda access-list extended uda_01
```

The following example deletes a UDA.

```
device# configure terminal
device(config)# no uda access-list extended uda_01
```

History

Release version	Command history
18s.1.00	This command was introduced.

uda-key

In a user-defined ACL (UDA)-profile, specifies up to four header fields for matching.

Syntax

uda-key0 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

uda-key1 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

uda-key2 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

uda-key3 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

no uda-key0 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

no uda-key1 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

no uda-key2 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

no uda-key3 header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } *header-field*

Command Default

No UDA key is specified.

Parameters

uda-key{0 | 1 | 2 | 3 }
: Specifies 1 through 4 UDA keys. You assign a header type and field to each key.

header{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 }
: Specifies a header type defined in the **flow** command.

header-field
: Specifies a supported field for one of the header types defined in the **flow** command. For fields supported for each header type, refer to Usage Guidelines.

Modes

UDA-profile configuration mode

Usage Guidelines

Ths command is supported only in NPB system mode.

You are not required to specify all four UDA keys. Keys not specified are programmed as match always (don't care).

You can specify fields from a header type in more than one UDA key.

A UDA starts functioning on an interface—for aggregation, replication, or forwarding—only if the following flow is implemented:

- Create a UDA profile, using the **uda-key profile** command.
- For the profile, specify the header types in the expected packet structure, using the **flow** command.

- For the profile, specify the header fields to match, using the **uda-key** command.
- Apply the profile to the interface, using the **uda-profile-apply** command.
- Create a UDA, using the **uda access-list** command.
- Create one or more permit or deny rules in the UDA, using the [**seq** *seq-value*] { **deny** | **permit** } command.
- Create a route-map, using the **route-map** command.
- Apply the UDA to the route-map, using the **match uda address acl** command.
- In the route-map, specify the egress interface, using the **set interface** or **set next-hop-tvf-domain** command.
- On a physical or port-channel interface, apply the route map to the ingress interface, using the **npb policy route-map** command.

To delete a UDA key, use the **no** form of this command.

To modify a key, delete the current key and define a new one.

The following tables display the fields supported for each header type:

TABLE 8 ETHERNET (Ethernet header)

Field	Width (Bits)	Description
HAS_INNER_TAG	1	Packet has inner tag?
HAS_OUTER_TAG	1	Packet has outer tag?
HAS_8021BR_TAG	1	Packet has 802.1BR tag?
HAS_VNTAG	1	Packet has VN tag?
ETHER_TYPE	16	EtherType
INNER_VID	16	PCP or DEI or VLAN ID
OUTER_VID	16	PCP or DEI or VLAN ID
8021BR_TAG	32	802.1BR tag
VNTAG	32	VN tag
MAC_SA_16_47	32	Bits 16–47 of SA MAC
MAC_SA_0_15	16	Bits 0–15 of SA MAC
MAC_DA_32_47	16	Bits 32–47 of DA MAC
MAC_DA_0_31	32	Bits 0–31 of DA MAC

TABLE 9 TUN_ETHERNET (Inner Ethernet header in tunneled frames)

Field	Width (Bits)	Description
HAS_INNER_TAG	1	Packet has inner tag?
HAS_OUTER_TAG	1	Packet has outer tag?
ETHER_TYPE	16	EtherType
INNER_VID	16	PCP or DEI or VLAN ID
OUTER_VID	16	PCP or DEI or VLAN ID
MAC_SA_16_47	32	Bits 16–47 of SA MAC
MAC_SA_0_15	16	Bits 0–15 of SA MAC
MAC_DA_32_47	16	Bits 32–47 of DA MAC
MAC_DA_0_31	32	Bits 0–31 of DA MAC

TABLE 10 IPV4 (IPv4 header)

Field	Width (Bits)	Description
DIP	32	Destination IP
SIP	32	Source IP
PROTOCOL	8	IP protocol
TOTAL_LENGTH	16	Total length
TOS	8	Type of service (DSCP & ECN)
ECN	2	ECN
DSCP	6	DSCP

TABLE 11 IPV6 (IPv6 header)

Field	Width (Bits)	Description
NEXT_HEADER	8	Next header
TOTAL_LENGTH	16	Total length
TRAFFIC_CLASS	8	Traffic class (DSCP & ECN)
ECN	2	ECN
DSCP	6	DSCP
DIP1	32	Bits 32-63 or 96-127 of Destination IP
DIP0	32	Bits 0-31 or 64-95 of Destination IP
SIP1	32	Bits 32-63 or 96-127 of Source IP
SIP0	32	Bits 0-31 or 64-95 of Source IP

TABLE 12 ARP (ARP header)

Field	Width (Bits)	Description
TARGET_IP	32	Target IP
TARGET_HW_ADDR_16_47	32	Bits 16-47 of target HW address
TARGET_HW_ADDR_0_15	16	Bits 0-15 of target HW address
SENDER_IP_16_31	16	Bits 16-31 of sender IP
SENDER_IP_0_15	16	Bits 0-15 of sender IP
SENDER_HW_ADDR_32_47	16	Bits 32-47 of sender HW address
SENDER_HW_ADDR_0_31	32	Bits 0-31 of sender HW address

TABLE 13 TCP (TCP header)

Field	Width (Bits)	Description
FLAGS	8	TCP flags
PORTS	32	Source and destination port
DST_PORT	16	Destination port
SRC_PORT	16	Source port

TABLE 14 UDP (UDP header)

Field	Width (Bits)	Description
PORTS	32	Source and destination port
DST_PORT	16	Destination port

TABLE 14 UDP (UDP header) (continued)

Field	Width (Bits)	Description
SRC_PORT	16	Source port

TABLE 15 SCTP (SCTP header)

Field	Width (Bits)	Description
PORTS	32	Source and destination port
DST_PORT	16	Destination port
SRC_PORT	16	Source port

TABLE 16 IGMP (IGMP header)

Field	Width (Bits)	Description
TYPE	8	Type

TABLE 17 ICMP (ICMP header)

Field	Width (Bits)	Description
TYPE_CODE	16	ICMP type and code

TABLE 18 ICMPV6 (ICMPv6 header)

Field	Width (Bits)	Description
TYPE_CODE	16	ICMPv6 type and code

TABLE 19 MPLS (MPLS header)

Field	Width (Bits)	Description
LABEL0	24	Label 0 (Label, EXP & S-Bit)
LABEL1	24	Label 1 (Label, EXP & S-Bit)
LABEL2	24	Label 2 (Label, EXP & S-Bit)
LABEL3	24	Label 3 (Label, EXP & S-Bit)

TABLE 20 GRE (GRE header)

Field	Width (Bits)	Description
IS_NVGRE	1	Packet has NVGRE encapsulation?
IS_ERSPAN	1	Packet has ERSPAN encapsulation?
IS_L2	1	Is payload L2?
IS_IPV4	1	Is payload IPv4?
IS_IPV6	1	Is payload IPv4?
FLAGS	8	First byte of the GRE header
KEY_24_31	8	Bits 24–31 of GRE key
KEY_0_23	24	Bits 0–23 of GRE key
TNI	24	NVGRE tenant network ID

TABLE 21 VXLAN (VXLAN header)

Field	Width (Bits)	Description
VNI	24	VXLAN network identifier

TABLE 22 GTP (GTP header)

Field	Width (Bits)	Description
TEID	32	GTP tunnel endpoint ID

TABLE 23 PAYLOAD4 (4 bytes)

Field	Width (Bits)	Description
WORD0	32	Word 0 in the payload

TABLE 24 PAYLOAD8 (8 bytes)

Field	Width (Bits)	Description
WORD0	32	Word 0 in the payload
WORD1	32	Word 1 in the payload

TABLE 25 PAYLOAD16 (16 bytes)

Field	Width (Bits)	Description
WORD0	32	Word 0 in the payload
WORD1	32	Word 1 in the payload
WORD2	32	Word 2 in the payload
WORD3	32	Word 3 in the payload

TABLE 26 PAYLOAD32 (32 bytes)

Field	Width (Bits)	Description
WORD0	32	Word 0 in the payload
WORD1	32	Word 1 in the payload
WORD2	32	Word 2 in the payload
WORD3	32	Word 3 in the payload
WORD4	32	Word 4 in the payload
WORD5	32	Word 5 in the payload
WORD6	32	Word 6 in the payload
WORD7	32	Word 7 in the payload

Examples

The following example configures a UDA profile, creates a flow, and specifies header types and fields.

```
device(config)# uda-key profile fkp1
device(conf-uda-profile-fkp1)# flow header0 ETHERNET header1 IPV4 header2 UDP header3 PAYLOAD32
device(conf-uda-profile-fkp1)# uda-key0 header0 ETHER_TYPE
device(conf-uda-profile-fkp1)# uda-key1 header1 PROTOCOL
device(conf-uda-profile-fkp1)# uda-key2 header2 DST_PORT
device(conf-uda-profile-fkp1)# uda-key3 header3 WORD1
```

History

Release version	Command history
18s.1.00	This command was introduced.

uda-key profile

Creates a user-defined ACL (UDA) profile, which specifies packet header fields for filtering.

Syntax

uda-key profile *profile-name*

no uda-key profile *profile-name*

Command Default

No UDA profile is defined.

Parameters

profile-name

Specifies a unique UDA-profile name. Valid names range from 1 through 63 characters.

Modes

Global configuration mode

Usage Guidelines

Ths command is supported only in NPB system mode.

A UDA starts functioning on an interface—for aggregation, replication, or forwarding—only if the following flow is implemented:

- Create a UDA profile, using the **uda-key profile** command.
- Configure the profile, using the **flow** and **uda-key** commands.
- Apply the profile to the interface, using the **uda-profile-apply** command.
- Create a UDA, using the **uda access-list** command.
- Create one or more permit or deny rules in the UDA, using the [**seq** *seq-value*] { **deny** | **permit** } command.
- Create a route-map, using the **route-map** command.
- Apply the UDA to the route-map, using the **match uda address acl** command.
- In the route-map, specify the egress interface, using the **set interface** or **set next-hop-tvf-domain** command.
- On a physical or port-channel interface, apply the route map to the ingress interface, using the **npb policy route-map** command.

To delete a UDA profile that is not applied to any interfaces, use the **no** form of this command.

Examples

The following example defines a UDA profile.

```
device# configure terminal
device(config)# uda-key profile prof_01
device(config-uda-key)#
```

The following example deletes a UDA profile.

```
device# configure terminal
device(config)# no uda-key profile prof_01
```

History

Release version	Command history
18s.1.00	This command was introduced.

uda-profile-apply

Applies a UDA profile to an Ethernet or port-channel interface.

Syntax

uda-profile-apply *profile-name*

no uda-profile-apply *profile-name*

Command Default

No UDA profile is applied.

Parameters

profile-name

Specifies a unique UDA-profile name. Valid names range from 1 through 63 characters.

Modes

Ethernet interface configuration mode

Port-channel configuration mode

Usage Guidelines

You can apply a UDA profile only to an Ethernet or to a port-channel interface.

It is not sufficient for a UDA to be applied to an interface—in a route-map. Unless a UDA-key profile is also applied to that interface, traffic on that interface is programmed as match-always.

To remove a UDA profile from an interface, use the **no** form of this command.

Examples

The following example applies a UDA profile to an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# uda-profile-apply prof_01
```

The following example removes a UDA profile from an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no uda-profile-apply prof_01
```

History

Release version	Command history
18s.1.00	This command was introduced.

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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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*

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

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.

The **no** form of the command restores the default of 5 seconds.

Examples

The following 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 will automatically turn 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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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%
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 USB storage 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

The following example removes a configuration file from a USB device attached to the local device.

```
device# usb remove directory config file startup-config.backup
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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 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 device.

```
device# configure terminal
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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"
```

History

Release version	Command history
17s.1.00	This command was introduced.

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** }] [**expire** { **never** | *YYYY-MM-DD* }]

no username *name*

Parameters

username
Specifies the account login name.

access-time *HHMM* **to** *HHMM*
Restricts the hours during the day that the user may be logged in. Valid values range from 0000 through 2400. By default, users are granted 24 hour access. Use 24-hour format. 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*
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 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 password expiration setting.

never
(Default) Does not specify a password expiration date.

YYYY-MM-DD
Specifies a password expiration date.

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 username account.

encryption-level { 0 | 7 }

Specifies the password encryption level. The values are 0 (clear text) and 7 (encrypted). Clear text (0) is the default. If service password-encryption is enabled, it overrides a user-level setting.

Modes

Global configuration mode

Usage Guidelines

The *username* must be from 1 through 40 characters. It must begin with a letter or underscore and be comprised of only letters, numbers, underscore and period. A username is case sensitive. It 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 **username** *username*, followed by the new values.

The maximum number of user accounts on a device is 64.

If a user's password, access time, or role is changed, any login sessions for that user are terminated.

To specify **access-time**, use the system time defined for the SLX-OS operating system. For the current system time, enter **show clock**.

To delete a user, enter the **no username** *username* command.

Examples

The following example configures a user account.

```
device# configure terminal
device(config)# username testUser password ******** role user desc
```

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 18:00 PM.

```
device# configure terminal
device(config)# username testUser access-time 0800 to 1800
```

History

Release version	Command history
17s.1.00	This command was introduced.

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# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 0/6
device(conf-if-eth-0/6)# 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# configure terminal
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# 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)# virtual-ip 2001:2019:8192::1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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 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 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)# protocol vrrp-extended
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
```

History

Release version	Command history
17s.1.00	This command was introduced.

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)#
```

History

Release version	Command history
17s.1.01	This command was introduced.

vlan (EVPN)

Specifies a VLAN in Ethernet Private Virtual Network (EVPN) mode, enters EVPN VLAN configuration mode, and adds or removes VLANs.

Syntax

vlan *vlan_id* [**add**|**remove**]

no vlan *vlan_id*]

Command Default

No VLAN is configured.

Parameters

vlan_id

Specifies a VLAN ID for the EVPN instance. Range is from 1 through 4090.

add

Adds a VLAN ID or range of VLAN IDs to the EVPN instance. Range is from 1 through 4090.

add

Adds a VLAN ID or range of VLAN IDs to the EVPN instance. Range is from 1 through 4090.

Modes

EVPN instance configuration mode

Usage Guidelines

Use the **no** form of this command to delete a VLAN from the EVPN instance.

Examples

To configure VLAN 10 and enter EVPN VLAN configuration mode:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# vlan 10
device(epvn-vlan-10)#
```

To add a VLAN to the EVPN instance:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# vlan add 20
```

To remove a range of VLANs from the EVPN instance:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# vlan remove 30-40
```

To delete a VLAN from the EVPN instance:

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# no vlan 10
```

History

Release version	Command history
	This command was introduced.
	This command was modified to...

vlan dot1q tag native

Enables 802.1Q tagging on the native VLAN on all trunked ports on the switch.

Syntax

vlan dot1q tag native

no vlan dot1q tag native

Command Default

The native VLAN is enabled.

Modes

Global configuration mode

Usage Guidelines

Usually, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN.

To maintain the tagging on the native VLAN and drop untagged traffic, use the **vlan dot1q tag native** command. The switch will tag the traffic received on the native VLAN and admit only 802.1Q-tagged frames.

Control traffic continues to be accepted as untagged on the native VLAN on a trunked port, even when the **vlan dot1q tag native** command is enabled.

Enter **no vlan dot1q tag native** to disable dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch.

History

Release version	Command history
17s.1.00	This command was introduced.

vrf

Creates a Virtual Routing and Forwarding (VRF) instance and enters VRF configuration mode.

Syntax

vrf *name*

Parameters

name

Character string for the name of the VRF. The string can be up 24 characters long, but should not contain punctuation or special characters.

Modes

Global configuration mode

Examples

To create the VRF instance "myvrf" and enter VRF configuration mode:

```
device# configure terminal
device(config)# vrf myvrf
device(config-vrf-myvrf)#
```

History

Release version	Command history
17s.1.00	This command was introduced.

vrf forwarding

Configures any port as a VRF port.

Syntax

vrf forwarding *vrf_name*

no vrf forwarding *vrf_name*

Parameters

vrf_name

The name of the VRF option for the port.

Command Default

By default, the out-of-band (OOB) management port (the eth0 interface) is part of the pre-defined VRF named mgmt-vrf.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of this command disables this VRF.

Examples

To enable the management VRF on an Ethernet interface and assign the interface to a subnet:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# vrf forwarding mgmt-vrf
device(conf-if-eth-0/1)# ip addr 10.1.1.1/24
```

To disable a management VRF previously configured on a VE interface:

```
device(config)# interface ve 100
device(conf-Ve-100)# no vrf forwarding mgmt-vrf
```

History

Release version	Command history
17s.1.00	This command was introduced.

vrf mgmt-vrf

Configures routes on a management VRF port.

Syntax

vrf mgmt-vrf

no vrf mgmt-vrf

Command Default

None

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables the management VRF.

The management VRF is a dedicated, secure VRF instance that allows users to manage the router inband on switched virtual interfaces (SVIs) and physical interfaces. The name of this VRF instance is "mgmt-vrf;" this instance cannot be deleted.

A management port is any port that is part of the management VRF. The OOB port cannot be removed from the management VRF. In addition, Layer 3 virtual and physical ports (also known as front-end or inband ports) can be part of the management VRF. Inband ports can be moved, by means of the CLI, into and out of the management VRF.

Examples

The following configures an IPv4 route subnet for the management VRF, enters address family IPv4 configuration mode, and assigns the management VRF to an Ethernet interface.

```
device# configure terminal
device(config)# vrf mgmt-vrf
device(config-vrf-mgmt-vrf)# ip route 10.1.1.0/32 ethernet 0/1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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

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# configure terminal
device(config)# protocol vrrp-extended
device(config)# interface ve 20
device(config-ve-20)# vrrp-extended-group 1
```

History

Release version	Command history
17s.1.00	This command was introduced.

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# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 0/6
device(conf-if-eth-0/6)# 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# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 0/6
device(conf-if-eth-0/6)# vrrp-group 1 version 3
```

History

Release version	Command history
17s.1.00	This command was introduced.

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.
!
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]:
```

History

Release version	Command history
17s.1.00	This command was introduced.