BROCADE

COMMAND REFERENCE GUIDE

NetIron Command Line Interface (CLI) Reference Guide, 06.0.00b

Supporting NetIron OS 06.0.00b

53-1004199-04
19 December 2016

© 2016, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, and MyBrocade are registered trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands, product names, or service names mentioned of Brocade Communications Systems, Inc. are listed at www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html. Other marks may belong to third parties.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

Preface **23**
- Document conventions 23
  - Notes, cautions, and warnings 23
  - Text formatting conventions 23
  - Command syntax conventions 24
- Brocade resources 24
- Document feedback 24
- Contacting Brocade Technical Support 25
  - Brocade customers 25
  - Brocade OEM customers 25

About This Document **27**
- What's new in this document 27
  - New commands 27
  - Modified commands 27
  - Deprecated commands 27
- Supported hardware and software 27

Using the NetIron Command-Line Interface **29**
- Logging on through the CLI 29
  - On-line help 29
  - Command completion 30
  - Scroll control 30
  - Line editing commands 30
- Command configuration modes 31
  - User EXEC mode 31
  - Privileged EXEC mode 31
  - Global configuration mode 31
  - Configuration modes 31
  - Accessing the CLI 32
  - Single user in global configuration mode 33
  - Multi-user conflict during deletion of group configuration (or stanza) 34
  - Navigating among command levels 34
- CLI command structure 34
  - Required or optional fields 35
  - Optional fields 35
  - List of available options 35
- Searching and filtering output 35
  - Searching and filtering output from show commands 36
  - Searching and filtering output at the --More-- prompt 37
  - Using special characters in regular expressions 38
- Allowable characters for LAG names 40
- CLI parsing enhancement 40
- Syntax shortcuts 40
- Saving configuration changes 41
  - Modifying startup and running configuration file manually 41

Commands A - E **43**

access-list....43
access-list (sequence)....46
activate (VRRP)....50
activate (VSRP)....51
additional-paths....52
additional-paths select....54
address-family multicast (BGP)....56
address-family unicast (BGP)....57
address-family unicast (IS-IS)....58
adjacency-check....59
adjustment-threshold....60
advertise backup....62
advertise backup (vsrp)....63
advertise-best-external....64
advertise-fec....65
aggregate-address (BGP)....66
always-compare-med....68
area authentication....69
area nssa (OSPFv2)....71
area nssa (OSPFv3)....73
area prefix-list (OSPFv2)....75
area range (OSPFv2)....77
area range (OSPFv3)....79
area stub (OSPFv2)....81
area stub (OSPFv3)....83
area virtual-link (OSPFv2)....85
area virtual-link (OSPFv3)....87
area virtual-link authentication (OSPFv3)....89
arp....91
arp-guard....93
arp-guard-access-list....94
arp-guard-syslog-timer....95
as-path-ignore....96
authentication (IKEv2)....97
auth-check....98
auth-key....99
auth-mode....100
auto-bandwidth....101
autobw-threshold-table....103
auto-cost reference-bandwidth (OSPFv2)....104
auto-cost reference-bandwidth (OSPFv3)....106
auto-enroll....108
auto-shutdown-new-neighbors....109
backup....110
backup (VSRP)....112
backup-bw-best-effort....114
backup-hello-interval....115
backup-hello-interval (vsrp)....116
bandwidth....117
bandwidth-ceiling....118

bandwidth-ceiling max threshold percentage 120
base vrf 121
bfd 122
bfd all-interfaces 124
bfd holdover-interval 126
bfd interval 128
bfd-enable 129
bfd mh-session-setup-delay 130
bfd sh-session-setup-delay 131
cam ifsr 132
cam-mode amod 134
capability as4 136
clear access-list receive accounting 137
clear arp-guard-statistics 138
clear bm histogram 140
clear cpu histogram sequence 141
clear dot1x-mka statistics 142
clear ikev2 statistics 143
clear ikev2 sa 144
clear ip bgp dampening 145
clear ip bgp flap-statistics 146
clear ip bgp local routes 147
clear ip bgp neighbor 148
clear ip bgp routes 150
clear ip bgp traffic 151
clear ip bgp vrf 152
clear ip ospf 153
clear ip vrrp statistics 155
clear ip vrrp-extended statistics 156
clear ipsec error-count 157
clear ipsec sa 158
clear ipsec statistics 159
clear ipsec statistics tunnel 160
clear ipv6 bgp dampening 161
clear ipv6 bgp flap-statistics 162
clear ipv6 bgp local routes 163
clear ipv6 bgp neighbor 164
clear ipv6 bgp routes 166
clear ipv6 bgp traffic 167
clear ipv6 ospf 168
clear ipv6 vrrp statistics 170
clear ipv6 vrrp-extended statistics 171
clear isis shortcut 172
clear mac-address vpls 173
clear macsec statistics 175
clear memory histogram 176
clear metro mp-vlp-queue 177
clear mmrp statistics 178
clear mpls auto-bandwidth-samples 179
clear mpls ldp neighbor 180

clear mpls ldp statistics....182
clear mpls rsvp statistics session....183
clear mpls statistics....185
clear mvrp statistics....188
clear openflow....189
clear pki counters....190
clear pki crl....191
clear rate-limit counters bum-drop....192
clear rate-limit counters ip-option-pkt-to-cpu....193
clear rate-limit counters ipv6-hoplimit-expired-to-cpu....194
clear rate-limit counters ip-ttl-expired-to-cpu....195
clear statistics openflow....196
client-interfaces sync_ccep_early....197
cluster-client-static-mac-move....198
cluster-id....199
copy....200
copy tftp license....202
copy-received-cos....203
common-name....204
compare-med-empty-aspath....205
compare-routerid....206
confederation identifier....207
confederation peers....208
cos....209
country-name....210
crl-query....211
crl-update-time....212
crypto key generate....213
crypto key zeroize....215
csnp-interval....216
cspf-computation-mode....217
cspf-computation-mode (LSP level)....219
database-overflow-interval (OSPFv2)....221
database-overflow-interval (OSPFv3)....222
dead-interval....223
dead-interval (vsrp)....225
default-information-originate (IS-IS)....226
default-information-originate (OSPFv2)....227
default-information-originate (OSPFv3)....229
default-link-metric....231
default-local-preference....233
default-metric (IS-IS)....234
default-metric (OSPF)....235
default-passive-interface....236
delete-certificate....237
deny (IPv6 ACL rules)....238
diagnostics (MRP)....243
disable authenticate md5....244
disable-acl-for-6to4....245
disable-acl-for-gre....247

disable-incremental-spf-opt ... 249
disable-inc-stct-spf-opt ... 250
disable-partial-spf-opt ... 251
distance (BGP) ... 252
distance (IS-IS) ... 253
distance (OSPF) ... 254
distribute-list prefix-list (OSPFv3) ... 256
distribute-list route-map ... 258
display-pkt-bit-rate ... 259
dot1ag-transparent ... 260
dot1x-key ... 261
dot1x-mka-enable ... 262
eckeypair ... 263
egress-truncate ... 264
egress-truncate-size ... 265
email ... 266
enable-mka ... 267
enable (VSRP) ... 269
enable-qos-statistics ... 269
encapsulation-mode ... 272
encryption ... 273
end-of-lib ... 274
enforce-first-as ... 275
enrollment ... 276
enrollment terminal ... 278
esn-enable ... 279
exclude-interface ... 280
export-vrf-leaked-routes ... 282
external-lsdb-limit (OSPFv2) ... 283
external-lsdb-limit (OSPFv3) ... 284
ext-stats-mode slot ... 285
extended-qos-mode set-force-tc-match-label-exp ... 287

Commands F - J ... 289

fast-external-fallover ... 289
fast-flood ... 290
fec-128-for-auto-discovered-peers ... 291
filter-fec ... 292
fingerprint ... 294
fqdn ... 295
garp-ra-interval ... 296
gig-default ... 297
graceful-restart (LDP) ... 299
graceful-restart (OSPFv2) ... 301
graceful-restart helper (OSPFv3) ... 303
graceful-restart helper-disable (IS-IS) ... 304
group-master interface ... 305
hello-interval (LDP) ... 307
hello-interval (VRRP) ... 309
hello-interval (VSRP) ... 311
hello-time ... 312

hello-timeout (LDP) 313
hello padding 315
hold-down-interval 316
hostname 317
ike-profile 318
ikev2 auth-proposal 319
ikev2 cookie-challenge 320
ikev2 dhgroup 321
ikev2 exchange-max-time 322
ikev2 http-url-cert 323
ikev2 limit 324
ikev2 nat-enable 325
ikev2 nat-keepalive 326
ikev2 policy 327
ikev2 profile 328
ikev2 proposal 330
ikev2 retransmit-interval 331
ikev2 retry-count 332
ike-profile 333
include-port 334
ingress-tunnel-accounting 335
initial-contact-payload 336
initial-ttl 337
In-label 338
install-igp-cost 339
integrity 340
ip 341
ip access-group 342
ip access-group enable-deny-logging 344
ip access-group enable-permit-logging 346
ip access-group redirect-deny-to-interf 348
ip access-group ve-traffic 349
ip access-list 350
ip access-list logging-age 352
ip allow-src-multicast 353
ip allow-src-multicast switched-traffic 354
ip arp-refresh-request-timer 355
ip host 356
ip http client connection timeout connect 357
ip http client connection timeout idle 358
ip http client source-interface 359
ip icmp fast-echo-reply 360
ip multicast-routing fast-convergence 362
ip multicast-routing optimization mct-scaling 363
ip match-payload-len 364
ip multicast-routing load-sharing 366
ip ospf active 367
ip ospf area 368
ip ospf auth-change-wait-time 369
ip ospf authentication-key 370

ip ospf bfd 371
ip ospf cost 372
ip ospf database-filter 373
ip ospf dead-interval 375
ip ospf hello-interval 376
ip ospf md5-authentication 377
ip ospf mtu-ignore 379
ip ospf network 380
ip ospf passive 382
ip ospf priority 383
ip ospf retransmit-interval 384
ip ospf transmit-delay 385
ip rate-limit option-pkt-to-cpu policy-map 386
ip rate-limit ttl-expired-to-cpu policy-map 388
ip receive access-list 390
ip receive access-list enable-permit-logging 392
ip route bfd 394
ip route static-bfd 396
ip router isis 398
ip ssh encryption disable-aes-cbc 399
ip tcp adjust-mss 400
ip tcp redirect-gre-tcp-syn 402
ip vrrp auth-type 404
ip vrrp vrid 406
ip vrrp-extended auth-type 407
ip vrrp-extended vrid 409
ip-address 410
ip-address (VSRP) 412
ipsec profile 413
ipsec proposal 414
ipsec self-sa-learning-enable 415
ipv6 access-list 416
ipv6-address 418
ipv6 dhcp-relay include-options 420
ipv6 match-payload-len 422
ipv6 mroute 424
ipv6 mroute next-hop-enable-default 426
ipv6 mroute next-hop-recursion 427
ipv6 multicast-routing load-sharing rebalance 428
ipv6 multicast-routing optimization mct-scaling 429
ipv6 nd proxy 430
ipv6 nd ra-dns-server 431
ipv6 nd ra-domain-name 432
ipv6 ospf active 434
ipv6 ospf area 435
ipv6 ospf authentication ipsec 436
ipv6 ospf authentication ipsec disable 437
ipv6 ospf authentication ipsec spi 438
ipv6 ospf bfd 440
ipv6 ospf cost 441

ipv6 ospf dead-interval 442
ipv6 ospf hello-interval 443
ipv6 ospf hello-jitter 444
ipv6 ospf instance 445
ipv6 ospf mtu-ignore 446
ipv6 ospf network 447
ipv6 ospf passive 448
ipv6 ospf priority 449
ipv6 ospf retransmit-interval 450
ipv6 ospf suppress-linklsa 451
ipv6 ospf transmit-delay 452
ipv6 rate-limit hoplimit-expired-to-cpu 453
ipv6 receive access-list 455
ipv6 receive access-list enable-deny-logging 457
ipv6 receive access-list enable-permit-logging 459
ipv6 receive deactivate-acl-all 460
ipv6 receive delete-acl-all 461
ipv6 receive rebind-acl-all 462
ipv6 route 463
ipv6 route bfd 466
ipv6 route next-hop 468
ipv6 route next-hop-enable-default 469
ipv6 next-hop-recursion 470
ipv6 route static-bfd 471
ipv6 router ospf 473
ipv6 router vrrp 474
ipv6 router vrrp-extended 475
ipv6 traffic-filter 476
ipv6 traffic-filter enable-deny-logging 478
ipv6 traffic-filter enable-permit-logging 480
ipv6 vrrp vrid 482
ipv6 vrrp-extended vrid 483
isis auth-check 484
isis auth-key 485
isis auth-mode 486
isis bfd 487
isis circut-type 488
isis hello padding 489
isis hello-interval 490
isis hello-multiplier 491
isis ipv6 metric 492
isis metric 493
isis passive 494
isis point-to-point 495
isis priority 496
isis reverse-metric 497
is-type 499
jitc enable 501

Commands K - Sh 503

ka-int-count 503

ka-interval....504
ka-timeout....505
key-add-remove-interval....506
key-rollover-interval....507
key-server-priority....509
l2 policy route-map....510
label-range static....512
key-rollover-interval....513
label-withdrawal-delay....515
lacp system-priority....516
lag port-primary-dynamic....517
ldp....518
ldp-enable....519
ldp-params....520
ldp-sync....521
License add....523
license delete....524
link-protection....525
link-redundancy....526
local-as....527
load-balance mask ip....528
load-balance mask ipv6....530
load-sharing....532
local-certificate....533
location....534
log (OSPFv2)....535
logging enable....537
log adjacency....540
log-dampening-debug....541
log invalid-lsp-packets....542
log-status-change....543
logs-per-interval-per-mep-rmep....544
lsp....546
lsp-gen-interval....547
lsp-interval....548
lsp-refresh-interval....549
lsr-id....550
mac access-group....551
mac access-group enable-deny-logging....553
mac access-list....554
mac-age-time....556
mac-move-det-syslog....558
macsec cipher-suite....560
macsec confidentiality-offset....562
macsec frame-validation....564
macsec replay-protection....565
match additional paths advertise-set....566
match identity....568
match l2acl....570
maximum-paths (IS-IS)....571

max-lsp-lifetime 572
max-metric router-lsa (OSPFv2) 573
max-metric router-lsa (OSPFv3) 575
med-missing-as-worst 577
method 578
metric 579
metric-style wide 580
metric-type 581
metro-ring 582
mka-auth-fail-action 583
mka-cfg-group 584
mmrp enable 585
mmrp include-vlan 586
mmrp point-to-point 587
mmrp registration-mode 588
mmrp timer 589
mpls-interface 590
multi-topology 591
mvrp applicant-mode 592
mvrp enable 593
mvrp point-to-point 594
mvrp registration-mode forbidden 595
mvrp timer 596
neighbor bfd 597
neighbor additional-paths 599
neighbor additional-paths advertise 601
neighbor additional-paths disable 603
neighbor ebgp-btsh 605
neighbor fail-over 607
neighbor next-hop-self (BGP) 609
net 610
next-hop-mpls 611
non-preempt-mode 613
non-preempt-mode (VRRP) 614
nonstop-routing (IS-IS) 615
nonstop-routing (OSPF) 616
notification-timer 617
ocsp-url 618
openflow controller source-interface 619
openflow enable 621
openflow hello-reply disable 623
org-name 625
org-unit-name 626
owner 627
partial-spf-interval 629
permit (arp-guard-access-list) 630
permit (IPv6 ACL rules) 631
pim neighbor-filter 636
ping mpls ldp 637
pki authenticate 639

pki cert validate 642
pki enroll 643
pki entity 645
pki export 646
pki export crl 647
pki export key 648
pki import 649
pki import key ec 652
pki profile-enrollment 653
pki trustpoint 655
pki-entity 656
port 657
port-primary-dynamic 658
pre-shared-key 661
pre-shared-key (IKEv2) 663
preforwarding-time 665
prf 667
protected 668
radius-server host 669
rate-limit exclude-ethernet-overhead 670
rate-limit input 672
rate-limit output 677
rate-limit strict-acl 681
rd 682
redistribute 683
remove-tagged-ports / remove-untagged-ports 686
remove-vlan 687
restart-ports 688
retransmit-interval 689
reverse-metric 690
revocation-check 692
rfc1583-compatibility (OSPF) 693
ring-interface 695
router-interface 696
router isis 697
router mpls 698
router ospf 699
router vrrp 700
router vsrp 701
router vrrp-extended 702
rpf shortcut 703
rsvp 704
rsvp-hello 705
rsvp-hello acknowledgments 707
rsvp-hello disable 708
rx-label-silence-time 713
sample-recording 714
scale-timer 716
scale-timer mrp 717
scp 718

session....719
set-debug....721
set-overload-bit....722
set next-hop-ip-tunnel....724
set next-hop-lsp....726
set next-hop-tvf-domain....727
sflow null0-sampling....728
shortcuts isis....729
shortcuts ospf....731
short-path-forwarding....732

Show Commands....733
show access-list accounting....733
show access-list bindings....736
show access-list receive accounting....737
show acl-policy....738
show arp....739
show arp-guard-access-list....741
show arp-guard port-bindings....743
show arp-guard statistics ethernet....745
show bfd....747
show bfd applications....749
show bfd mpls....750
show bfd neighbors....751
show bfd neighbors bgp....753
show bfd neighbors details....757
show bfd neighbors interface....760
show bfd neighbors isis....761
show bfd neighbors ospf....762
show bfd neighbors ospf6....763
show bfd neighbors static....764
show bfd neighbors static6....765
show bip slot....766
show cam-detail-eth....768
show cam-detail-ip....771
show cam ifl....773
show cam ipvpn....775
show cam uda....777
show cluster....778
show configuration....783
show cpu histogram....784
show cpu histogram sequence....787
show dot1x-mka group....789
show dot1x-mka config....791
show dot1x-mka sessions brief....793
show dot1x-mka sessions ethernet....794
show dot1x-mka statistics....798
show egress-truncate....800
show flow-ctrl....802
show ikev2 policy....804
show ikev2 profile....806

show ikev2 proposal 808
show ikev2 sa 810
show ikev2 session 812
show ikev2 statistics 814
show interface ethernet 816
show interfaces tunnel 818
show ip allow-src-multicast 820
show ip bgp 821
show ip bgp attribute-entries 822
show ip bgp config 824
show ip bgp dampened-paths 825
show ip bgp filtered-routes 826
show ip bgp flap-statistics 827
show ip bgp ipv6 829
show ip bgp neighbors 832
show ip bgp neighbors advertised-routes 839
show ip bgp neighbors flap-statistics 840
show ip bgp neighbors last-packet-with-error 841
show ip bgp neighbors received 842
show ip bgp neighbors received-routes 843
show ip bgp neighbors rib-out-routes 844
show ip bgp routes community 845
show ip bgp neighbors routes 846
show ip bgp neighbors routes-summary 847
show ip bgp peer-group 850
show ip bgp routes 851
show ip bgp summary 855
show ip bgp vrf neighbors 858
show ip bgp vrf routes 860
show ip bgp vrf 862
show ip http client 864
show ip icmp fast-echo-reply 866
show ip icmp vrf fast-echo-reply 869
show ip igmp cluster-client 873
show ip igmp group count 874
show ip pim counter mct 875
show ip pim global 877
show ip interface 878
show ip match-payload-len 882
show ip pim global 884
show ip mbgp ipv6 885
show ip multicast 887
show ip multicast vpls 891
show ip ospf 894
show ip ospf area 895
show ip ospf border-routers 897
show ip ospf config 898
show ip ospf database 901
show ip ospf interface 905
show ip ospf neighbor 909

show ip ospf redistribute route 912
show ip ospf routes 913
show ip ospf summary 916
show ip ospf traffic 917
show ip ospf trap 918
show ip ospf virtual link 919
show ip ospf virtual neighbor 920
show ip route 921
show ip static-arp 924
show ip vrrp 926
show ip vrrp-extended 929
show ipsec egress-config 934
show ipsec egress-spi-table 935
show ipsec error-count 936
show ipsec ingress-config 937
show ipsec ingress-spi-table 938
show ipsec policy 939
show ipsec profile 940
show ipsec proposal 942
show ipsec sa 944
show ipsec statistics 946
show ip-tunnels 948
show ipv6 access-list bindings 950
show ipv6 access-list receive accounting 951
show ipv6 bgp 952
show ipv6 bgp attribute-entries 954
show ipv6 bgp config 956
show ipv6 bgp dampened-paths 957
show ipv6 bgp filtered-routes 958
show ipv6 bgp flap-statistics 961
show ipv6 bgp neighbors 963
show ipv6 bgp neighbors advertised-routes 969
show ipv6 bgp neighbors flap-statistics 971
show ipv6 bgp neighbors last-packet-with-error 972
show ipv6 bgp neighbors received 973
show ipv6 bgp neighbors received-routes 974
show ipv6 bgp neighbors rib-out-routes 977
show ipv6 bgp neighbors routes 979
show ipv6 bgp neighbors routes-summary 982
show ipv6 bgp nexthop 984
show ipv6 bgp peer-group 985
show ipv6 bgp routes 986
show ipv6 bgp routes community 990
show ipv6 bgp summary 991
show ipv6 bgp vrf 994
show ipv6 bgp vrf neighbors 996
show ipv6 bgp vrf routes 998
show ipv6 bgp vrf routes community 1000
show ipv6 dhcp-relay interface 1001
show ipv6 dhcp-relay options 1002

show ipv6 interface tunnel 1003
show ipv6 match-payload-len 1005
show ipv6 mld cluster-client group 1007
show ipv6 pim counter mct 1008
show ipv6 pim global 1009
show ipv6 ospf 1010
show ipv6 ospf area 1011
show ipv6 ospf database 1013
show ipv6 ospf interface 1020
show ipv6 ospf memory 1026
show ipv6 ospf neighbor 1028
show ipv6 ospf redistribute route 1032
show ipv6 ospf routes 1034
show ipv6 ospf spf 1036
show ipv6 ospf summary 1039
show ipv6 ospf virtual-links 1040
show ipv6 ospf virtual-neighbor 1041
show ipv6 vrrp 1043
show ipv6 vrrp-extended 1047
show isis 1051
show isis config 1055
show isis counts 1056
show isis database 1059
show isis hostname 1062
show isis interface 1063
show isis ipv6 spf-log 1067
show isis neighbor 1069
show isis routes 1072
show isis shortcut 1074
show isis spf-log 1076
show isis traffic 1079
show license 1080
show load-balance mask-options 1082
show macsec ethernet 1084
show macsec statistics ethernet 1085
show memory histogram 1088
show metro mp-vlp-queue 1090
show metro-ring 1092
show mmrp 1095
show mmrp attributes 1097
show mmrp config 1099
show mmrp statistics 1100
show mpls autobw-threshold-table 1102
show mpls bypass-lsp 1103
show mpls config 1106
show mpls forwarding 1109
show mpls interface 1111
show mpls label-range 1113
show mpls ldp 1115
show mpls ldp database 1116

show mpls ldp fec....1118
show mpls ldp interface....1122
show mpls ldp neighbor....1124
show mpls ldp path....1126
show mpls ldp peer....1128
show mpls ldp session....1130
show mpls ldp statistics....1132
show mpls ldp tunnel....1134
show mpls lsp....1136
show mpls lsp_p2mp_xc....1143
show mpls path....1145
show mpls policy....1147
show mpls route....1150
show mpls rsvp interface....1152
show mpls rsvp neighbor....1154
show mpls rsvp session....1157
show mpls rsvp session backup....1162
show mpls rsvp session brief....1164
show mpls rsvp session bypass....1166
show mpls rsvp session destination....1168
show mpls rsvp session detail....1170
show mpls rsvp session detour....1172
show mpls rsvp session down....1174
show mpls rsvp session extensive....1176
show mpls rsvp session (ingress/egress)....1179
show mpls rsvp session (interface)....1181
show mpls rsvp session name....1182
show mpls rsvp session p2mp....1186
show mpls rsvp session p2p....1190
show mpls rsvp session ppend....1192
show mpls rsvp session transit....1194
show mpls rsvp session up....1196
show mpls rsvp session wide....1198
show mpls rsvp statistics....1200
show mpls static-lsp....1202
show mpls statistics 6pe....1205
show mpls statistics bypass-lsp....1206
show mpls statistics label....1207
show mpls statistics ldp transit....1209
show mpls statistics ldp tunnel....1211
show mpls statistics lsp....1213
show mpls statistics oam....1214
show mpls statistics vll....1215
show mpls statistics vll-local....1217
show mpls statistics vpls....1219
show mpls statistics vrf....1221
show mpls summary....1222
show mpls ted database....1224
show mpls ted path....1226
show mpls vll....1229

show mpls vll-local ... 1232
show mpls vpls ... 1234
show mstp ... 1240
show mvrp ... 1241
show mvrp attributes ... 1242
show mvrp config ... 1244
show mvrp statistics ... 1245
show nht-table ipsec-based ... 1247
show openflow ... 1248
show openflow controller ... 1249
show openflow flows ... 1250
show openflow groups ... 1252
show openflow interface ... 1254
show openflow meters ... 1256
show openflow queues ... 1258
show packet-encap-processing ... 1260
show packet-encap-processing slot ... 1262
show packet-encap-processing strip-802-1BR ... 1263
show packet-encap-processing strip-vn-tag ... 1264
show packet-encap-processing interface ethernet ... 1265
show pim interface ... 1266
show pim multicast-filter ... 1267
show pki certificates ... 1268
show pki counters ... 1271
show pki crls ... 1272
show pki enrollment-profile ... 1273
show pki entity ... 1274
show pki key mypubkey ... 1275
show pki trustpoint ... 1276
show rate-limit counters bum-drop ... 1278
show rate-limit detail ... 1280
show rate-limit interface ... 1281
show rate-limit ipv6 hoplimit-expired-to-cpu ... 1282
show rate-limit option-pkt-to-cpu ... 1283
show rate-limit ttl-expired-to-cpu ... 1284
show rmon alarm ... 1285
show rmon statistics ... 1286
show route-map ... 1288
show rstp ... 1289
show running-config ... 1291
show sflow statistics ... 1293
show spanning-tree ... 1294
show statistics ... 1296
show sysmon config ... 1300
show sysmon results brief ... 1301
show sysmon results detail ... 1303
show sysmon schedule ... 1305
show telemetry ... 1307
show terminal ... 1309
show tm-voq-stat queue-drops ... 1310

show tvf-domain ... 1311
show vlan ... 1315
show vlan tvf-lag-lb ... 1317
show vsrp ... 1318

Commands Si - Z ... 1321

slow-start ... 1321
slow-start ... 1323
snmp-server community ... 1324
snmp-server context ... 1326
snmp-server enable mib ... 1327
snmp-server enable traps ... 1328
snmp-server enable traps bum-rl-traps ... 1329
snmp-server host ... 1330
snmp-server mib community-map ... 1333
spanning-tree pvst-protect ... 1334
spf-interval ... 1336
state-name ... 1338
static-lsp ... 1339
static-mac-address ... 1340
statistics-load-interval ... 1341
strip-802-1br ... 1343
strip-vn-tag ... 1345
subject-alt-name ... 1347
summary-address ... 1349
summary-address (OSPFv2) ... 1350
summary-address (OSPFv3) ... 1352
summary-prefix ... 1354
suppress-acl-seq ... 1355
suppress-ipv6-priority-mapping ... 1356
sysmon fe link auto-tune ... 1357
sysmon ipc rel-q-mon enable ... 1358
sysmon lp-high-cpu enable ... 1359
sysmon lp-high-cpu threshold ... 1360
sysmon mp-high-cpu cpu-threshold ... 1361
sysmon mp-high-cpu enable ... 1362
sysmon mp-high-cpu task-threshold ... 1363
sysmon np memory-errors ... 1364
sysmon port port-crc-test ... 1367
sysmon sfm walk auto ... 1369
sysmon sfm walk polling-period ... 1370
sysmon sfm walk redundancy-check ... 1371
sysmon sfm walk start ... 1372
sysmon sfm walk status ... 1373
sysmon sfm walk stop ... 1375
sysmon sfm walk threshold ... 1376
sysmon tm link auto-tune ... 1378
system np control-ram-threshold ... 1379
system np lpm-ram-threshold ... 1381
system-init ... 1383
system-max ecmp-pram-block-size ... 1385

system-max ip-arp....1386
system-max ipv6-receive-cam....1387
system-max ipv6-vrf-route....1388
system-max ip-vrf-route....1389
system-max rstp....1390
system-max trunk-num....1391
system-max tvf-lag-lb-fid-group....1392
system-max tvf-lag-lb-fid-pool....1393
te-metric....1395
terminal enable timestamp....1396
timers (OSPFv2)....1399
timers (OSPFv3)....1401
traceroute....1403
traceroute mpls ldp....1405
track-port....1407
track-port (VSRP)....1409
transparent-hw-flooding lag-load-balancing....1410
transport-address interface....1411
tunnel destination....1412
tunnel mode ipsec ipv4....1413
tunnel mode ipsec ipv6....1414
tunnel override-pkt-tos-ttl....1415
tunnel protection ipsec profile....1416
tunnel source....1417
tunnel-interface....1418
tvf-domain....1420
tx-label-silence-timer....1421
uda access-group....1422
uda-offsets....1424
underflow-limit....1426
update-lag-name....1428
use-v2-checksum....1430
use-vrrp-path....1431
version....1432
virtual-mac....1433
vll....1434
vll-peer....1436
vrf forwarding....1439
vsrp....1440
vsrp auth-type....1441
vsrp restart-port....1442
write memory....1443

Preface

- Document conventions....23
- Brocade resources....24
- Document feedback....24
- Contacting Brocade Technical Support....25

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

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.
`Courier font`	Identifies CLI output.

Format	Description
	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.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	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. In Fibre Channel products, square brackets may be used instead for this purpose.
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.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade.
Click the **Support** tab and select **Document Library** to access documentation on MyBrocade or www.brocade.com You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.com

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.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online or by telephone. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone
Preferred method of contact for non-urgent issues: • Case management through the MyBrocade portal. • Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • Toll-free numbers are available in many countries. • For areas unable to access a toll-free number: +1-408-333-6061

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

About This Document

- What's new in this document....27
- Supported hardware and software....27

What's new in this document

This document is the NetIron Command Reference.

In this release of the NetIron command reference, not all commands supported on the NetIron devices are represented. All new commands supported in the NetIron OS 5.0.00, and later release, are included.

For new commands introduced since Release 6.0.00, the history table is shown. For legacy commands, the history table is not shown unless an update has been added in recent releases.

The following are lists of the new, modified, and deprecated commands in Release 6.0.00b:

New commands

The following commands have been added (new for this release).

- **<add commands here>**

Modified commands

There are no modified commands in this release.

Deprecated commands

There are no deprecated commands in this release.

Supported hardware and software

The hardware platforms in the following table are supported by this release of this guide.

TABLE 1 Supported devices

Brocade NetIron XMR Series	Brocade NetIron MLX Series	NetIron CES 2000 and NetIron CER 2000 Series
Brocade NetIron XMR 4000	Brocade MLX-4	Brocade NetIron CES 2024C
Brocade NetIron XMR 8000	Brocade MLX-8	Brocade NetIron CES 2024F
Brocade NetIron XMR 16000	Brocade MLX-16	Brocade NetIron CES 2048C
Brocade NetIron XMR 32000	Brocade MLX-32	Brocade NetIron CES 2048CX
	Brocade MLXe-4	Brocade NetIron CES 2048F
	Brocade MLXe-8	Brocade NetIron CES 2048FX
	Brocade MLXe-16	Brocade NetIron CER 2024C

TABLE 1 Supported devices (continued)

Brocade NetIron XMR Series	Brocade NetIron MLX Series	NetIron CES 2000 and NetIron CER 2000 Series
	Brocade MLXe-32	Brocade NetIron CER-RT 2024C Brocade NetIron CER 2024F Brocade NetIron CER-RT 2024F Brocade NetIron CER 2048C Brocade NetIron CER-RT 2048C Brocade NetIron CER 2048CX Brocade NetIron CER-RT 2048CX Brocade NetIron CER 2048F Brocade NetIron CER-RT 2048F Brocade NetIron CER 2048FX Brocade NetIron CER-RT 2048FX

Using the NetIron Command-Line Interface

- Logging on through the CLI....29
- Command configuration modes....31
- CLI command structure....34
- Searching and filtering output....35
- Allowable characters for LAG names....40
- CLI parsing enhancement....40
- Syntax shortcuts....40
- Saving configuration changes....41

Logging on through the CLI

After an IP address is assigned to the Brocade device's management port, you can access the CLI through a PC or terminal attached to the management module's serial (Console) port or 10BaseT/100BaseTX Ethernet (management) port, or from a Telnet or SSH connection to the PC or terminal.

You can initiate a local Telnet, SSH or SNMP connection by specifying the management port's IP address.

The commands in the CLI are organized into the following modes:

- **User EXEC mode** - Lets you display information and perform basic tasks such as pings and traceroutes.
- **Privileged EXEC mode** - Lets you use the same commands as those at the User EXEC level plus configuration commands that do not require saving the changes to the system-config file.
- **Global configuration mode** - Lets you make configuration changes to the device. To save the changes across software reloads and system resets, you need to save them to the system-config file. The global configuration mode contains sub-configuration modes for individual ports, for VLANs, for routing protocols, and other configuration areas.

  NOTE
  By default, the Brocade devices have all management access disabled, except for console port management. To create access, you must configure Enable passwords or local user accounts, or you can configure the device to use a RADIUS or TACACS or TACACS+ server for authentication.

On-line help

To display a list of available commands or command options, enter "?" or press Tab. If you have not entered part of a command at the command prompt, all the commands supported at the current CLI level are listed. If you enter part of a command, then enter "?" or press Tab, the CLI lists the options you can enter at this point in the command string.

If you enter an invalid command, a message appears indicating the command was unrecognized.

```
device(config)# rooter ip
Unrecognized command
```

Command completion

The CLI supports command completion, so you do not need to enter the entire name of a command or option. As long as you enter enough characters of the command or option name to avoid ambiguity with other commands or options, the CLI understands what you are typing.

Scroll control

By default, the CLI uses a page mode to paginate displays that are longer than the number of rows in your terminal emulation window. For example, if you display a list of all the commands at the global CONFIG level but your terminal emulation window does not have enough rows to display them all at once, the page mode stops the display and lists your choices for continuing the display.

```
aaa
access-list
all-client
arp
banner
base-mac-addr
boot
some lines omitted for brevity...
 default-vlan-id
 enable
 enable-acl-counter
 end
 exit
--More--, next page: Space, next line: Return key, quit: Control-c
```

The software provides the following scrolling options:

- Press the Space bar to display the next page (one screen at time).
- Press the Return or Enter key to display the next line (one line at a time).
- Press Ctrl-C cancel the display.

Line editing commands

The CLI supports the following line editing commands. To enter a line-editing command, use the CTRL+key combination for the command by pressing and holding the CTRL key, then pressing the letter associated with the command.

TABLE 2 CLI line editing commands

Ctrl+Key combination	Description
Ctrl+A	Moves to the first character on the command line.
Ctrl+B	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+D	Deletes the character at the cursor.
Ctrl+E	Moves to the end of the current command line.
Ctrl+F	Moves the cursor forward one character.
Ctrl+K	Deletes all characters from the cursor to the end of the command line.
Ctrl+L; Ctrl+R	Repeats the current command line on a new line.
Ctrl+N	Enters the next command line in the history buffer.
Ctrl+P	Enters the previous command line in the history buffer.
Ctrl+U; Ctrl+X	Deletes all characters from the cursor to the beginning of the command line.

TABLE 2 CLI line editing commands (continued)

Ctrl+Key combination	Description
Ctrl+W	Deletes the last word you typed.
Ctrl+Z	Moves from any CONFIG level of the CLI to the Privileged EXEC level; at the Privileged EXEC level, moves to the User EXEC level.

Command configuration modes

The Brocade 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.

User EXEC mode

User EXEC mode is the default mode for the device; it supports the lowest level of user permissions. In this mode, you can execute basic commands such as **ping** and **traceroute**, but only a subset of clear, show, and debug commands can be entered in this mode. The following example shows the User EXEC prompt after login. The **enable** command enters privileged EXEC mode.

```
device> enable
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 1/1
device(config-if-e1000-1/1)#
```

Configuration modes

Configuration command-line interface (CLI) commands are entered in various modes to configure a Brocade device. The initial configuration mode is named global configuration mode and all other configuration modes are accessed through this mode.

The following table displays a list of the most commonly-used sub-configuration modes, but this list is not exhaustive and new sub-configuration modes can be introduced with new features. Refer to the command pages for details of the configuration modes applicable to the CLI command and examples of how to access the required mode.

TABLE 3 Sub-configuration modes

Configuration mode	Description
802.1X port security	The 802.1X port security mode allows you to configure the 802.1X port security. You access this mode by entering the **dot1x-enable** command from global configuration mode.
BGP	The BGP mode allows you to configure Border Gateway Protocol version 4 (BGP4) features. You access this mode by entering the **router bgp** command from global configuration mode.
BGP4 unicast address family	The BGP4 unicast address family mode allows you to configure a BGP4 unicast route. You access this mode by entering the **address-family ipv4 unicast** command from BGP configuration mode.
BGP4 multicast address family	The BGP4 multicast address family mode allows you to configure BGP4 multicast routes. You access this mode by entering the **address-family ipv4 multicast** command from BGP configuration mode, BGP unicast address configuration mode, or IPv6 BGP unicast configuration mode.
Ethernet service instance	Ethernet Service Instance (ESI) mode allows you to assign an ESI to a protocol, or port.
Interface	The interface mode allows you to assign or modify specific port parameters on a specific port. You access this mode by entering the **interface** command followed by an appropriate keyword and variables from global configuration mode. Available keywords are: **ethernet**, **loopback**, **management**, **ve**, **tunnel**, or **group-ve**.
LAG	The LAG mode allows you to change parameters for statically-configured LAG groups. You access this mode by entering the **lag** command with appropriate port parameters from global configuration mode.
MAC port security	The MAC port security mode allows you to configure the port security feature. You reach this level by entering the **port security** command at the global or interface configuration mode.
Metro ring	The Metro ring mode allows you to configure Layer 2 connectivity and fast failover in ring topologies. You access this mode by entering the **metro-ring** command with a *ring-id* variable from VLAN configuration mode..
OSPF	The OSPF mode allows you to configure parameters for the OSPF routing protocol. You access this mode by entering the **router ospf** command from global configuration mode.
PIM	The PIM mode allows you to configure parameters for the Protocol Independent Multicast (PIM) routing protocol. You access this mode by entering the **router pim** command from global configuration mode.
Redundancy	The redundancy mode allows you to configure redundancy parameters for redundant management modules. You access this mode by entering the **redundancy** command from global configuration mode.
RIP	The RIP mode allows you to configure parameters for the RIP routing protocol. You access this mode by entering the **router rip** command from global configuration mode.
Route map	The route map mode allows you to configure parameters for a BGP4 route map. You access this mode by entering the **route-map** command with a *name* variable from global configuration mode.
Topology group	The topology group mode allows you to control the Layer 2 protocol configuration and Layer 2 state of a set of ports in multiple VLANs based on the configuration and states of those ports in a single master VLAN. One instance of the Layer 2 protocol controls all the VLANs. You access this mode by entering the **topology-group** command with a *group-id* variable from global configuration mode.
VLAN	Policy-based virtual Local Area Networks (VLANs) mode allow you to assign VLANs to a protocol, port, or 802.1q tags. You access this mode by entering the **vlan** command with a *vlan-id* variable from global configuration mode.
VSRP	The VSRP mode allows you to configure parameters for the Virtual Switch Redundancy Protocol (VSRP). You access this mode by entering the **vsrp vrid** command with a *num* variable from VLAN configuration mode.
VRRP	The VRRP mode allows you to configure parameters for the Virtual Router Redundancy Protocol (VRRP). You access this mode by entering the **router vrrp** command from global configuration mode and then entering the **ip vrrp vrid** command from interface configuration mode.
VRRP-E	The VRRP-E mode allows you to configure parameters for the VRRP Extended (VRRP-E) protocol. You access this mode by entering the **router vrrp-extended** command from global configuration mode and then entering the **ip vrrp-extended vrid** command from interface configuration mode.

Accessing the CLI

The CLI can be accessed through both serial and Telnet connections. For initial log on, you must use a serial connection. Once an IP address is assigned, you can access the CLI through Telnet.

Once connectivity to the device is established, you will see the a prompt.

```
device>
```

When accessing the CLI through Telnet, you maybe prompted for a password. By default, the password required is the password you enter for general access at initial setup. You also have the option of assigning a separate password for Telnet access with the **enable telnet password** *password* command, found at the Global Level.

At initial log on, all you need to do is type **enable** at the prompt, then press Return. You only need to enter a password after a permanent password is entered at the Global CONFIG Level of the CLI.

To reach the Global CONFIG Level, the uppermost level of the CONFIG commands, enter the following commands

device > enable	User Level commands
device # configure terminal	Privileged Level-EXEC commands
device (config)#	Global Level-CONFIG commands

You can then reach all other levels of the CONFIG command structure from this point.

The CLI prompt will change at each level of the CONFIG command structure, to easily identify the current level.

```
device> User Level EXEC Command
device# Privileged Level EXEC Command
device(config)# Global Level CONFIG Command
device(config-if-e10000-5/1)# Interface Level CONFIG Command
device(config-lbif-1)# Loopback Interface CONFIG Command
device(config-ve-1)# Virtual Interface CONFIG Command
device(config-trunk-4/1-4/8)#    trunk group CONFIG Command
device(config-if-e10000-tunnel)# IP Tunnel Level CONFIG Command
device(config-bgp-router)# BGP Level CONFIG Command
device(config-ospf-router)# OSPF Level CONFIG Command
device(config-isis-router)# IS-IS Level CONFIG Command
device(config-pim-router)# PIM Level CONFIG Command
device(config-redundancy)# Redundant Management Module CONFIG Command
device(config-rip-router)# RIP Level CONFIG Command
device(config-port-80)# Application Port CONFIG Command
device(config-bgp-routemap Map_Name)# Route Map Level CONFIG Command
device(config-vlan-1)# VLAN Port-based Level CONFIG Command
device(config-vlan-atalk-proto)# VLAN Protocol Level CONFIG Command
```

NOTE

The CLI prompt at the interface level includes the port speed. The speed is one of the following:device (config-if-e100-5/1)# - The interface is a 10/100 port.device (config-if-e1000-5/1)# - The interface is a Gigabit port.For simplicity, the port speeds sometimes are not shown in example Interface level prompts in this manual.

Single user in global configuration mode

By default, more than one user can enter the global configuration mode of a device CLI, which is accessed through the **configure terminal** command. While in global configuration mode, users can override another user's configuration changes.

You can configure a device to allow only one user to be in global configuration mode at any one time. Other users who try to enter that mode in will be denied. To allow only one user to enter global configuration mode, enter the following command.

```
device#configure terminal
device(config)# single-config-user
device(config)# write memory
```

Syntax: [no] single-config-user

After the **single-config-user** command is issued, the device will not allow more than one user to enter global configuration mode. However, if you run the command while more than one user is in global configuration mode, the other users continue to be in global configuration mode and can potentially override each other's configuration changes. Only users who try to enter the global configuration mode after the command is issued are prevented from entering global configuration mode. If a user is already in that mode and another user tries to enter global configuration mode after the **single-config-user** command is issued, the following error is displayed.

```
device#configure terminal
Single user config mode is being enforced. Config mode is being used by <session-type> session.
```

where *session-type* can be one of the following:

- **console**
- **telnet** *number*
- **SSH** *number*

Multi-user conflict during deletion of group configuration (or stanza)

By default, a user may delete a group configuration, even if another user is simultaneously in that mode. You can disable this feature by issuing the **enable multi-user-mode-deletion** command.

To allow only one user to delete group configurations, enter the following command.

```
device#configure terminal
device(config)# enable multi-user-mode-deletion
device(config)# write memory
```

When a user attempts to delete a group configuration from the CLI, and another user is already within that group configuration, the user who tries to delete a group configuration in that mode will be denied and will receive the following error message.

```
Session 1:
device(config)# vlan 10
device(config-vlan-10)#
Session 2:

device(config)# no vlan 10
"Error: Cannot undo the configuration as {console|telnet|SSH} session is       using this mode."
```

Syntax: [no] enable multi-user-mode-deletion

Use the **no** form of this command will allow multiple users the ability to delete group configurations.

NOTE
This feature will not work on commands that are issued from the WEB management and the SNMP management.

Navigating among command levels

To reach other CLI command levels, you need to enter certain commands. At each level there is a launch command that allows you to move either up or down to the next level.

CLI command structure

Many CLI commands may require textual or numeral input as part of the command.

Required or optional fields

These fields are either required or optional depending on how the information is bracketed. For clarity, a few CLI command examples are explained below.

Syntax: [no] deny redistribute *value* { **all** | **bgp** | **rip** | **static address** *ip-addr ip-mask* [**match-metric** *value* | **set-metric** *value*] }

When an item is in italics, the information requested is a variable and required.

When an item is not bracketed with "{ }" symbols, the item is a required keyword or variable.

When an item is bracketed with "{ }" symbols, one of the items separated by a vertical bar "|" must be chosen.

When an item is bracketed with "[ ]" symbols, the information requested is optional.

Optional fields

When two or more options are separated by a vertical bar, " | ", you must enter one of the options as part of the command.

Syntax: priority normal | **high**

For example, the "normal | high" entry in the Syntax above means that priority can be either priority normal or priority high. The command in the syntax above requires that you enter either normal or high as part of the command.

List of available options

To get a quick display of available options at a CLI level or for the next option in a command string, enter a question mark (?) at the prompt or press TAB.

To view all available commands at the user EXEC level, enter the following or press TAB at the User EXEC CLI level.

```
device> ?
enable
exit
fastboot
ping
show
stop-trace-route
traceroute
```

You also can use the question mark (?) with an individual command, to see all available options or to check context.

Enter the following to view possible **copy** command options.

```
device# copy ?
  flash
  running-config
  startup-config
  tftp
device# copy flash ?
  tftp
```

Searching and filtering output

You can filter CLI output from **show** commands and at the --More-- prompt. You can search for individual characters, strings, or construct complex regular expressions to filter the output.

Searching and filtering output from show commands

You can filter output from **show** commands to display lines containing a specified string, lines that do not contain a specified string, or output starting with a line containing a specified string. The search string is a regular expression consisting of a single character or string of characters. You can use special characters to construct complex regular expressions. Refer to the “Using special characters in regular expressions” section for information on special characters used with regular expressions.

Displaying lines containing a specified string

The following command filters the output of the **show interface** command for port 3/11 so it displays only lines containing the word "Internet". This command can be used to display the IP address of the interface.

```
device# show interface e 3/11 | include Internet
  Internet address is 192.168.1.11/24, MTU 1518 bytes, encapsulation ethernet
```

Syntax: show-command include | regular-expression

> NOTE
> The vertical bar (|) is part of the command.

Note that the regular expression specified as the search string is case sensitive. In the example above, a search string of "Internet" would match the line containing the IP address, but a search string of "internet" would not.

Displaying lines that do not contain a specified string

The following command filters the output of the **show who** command so it displays only lines that do not contain the word "closed". This command can be used to display open connections to the device.

```
device# show who | exclude closed
Console connections:
        established
        you are connecting to this session
        2 seconds in idle
Telnet connections (inbound):
 1      established, client ip address 192.168.9.37
        27 seconds in idle
Telnet connection (outbound):
SSH connections:
```

Syntax: show-command exclude | regular-expression

Displaying lines starting with a specified string

The following command filters the output of the **show who** command so it displays output starting with the first line that contains the word "SSH". This command can be used to display information about SSH connections to the Brocade device.

```
device# show who | begin SSH
SSH connections:
 1      established, client ip address 192.168.9.210
        7 seconds in idle
 2      closed
 3      closed
 4      closed
 5      closed
```

Syntax: show-command begin | regular-expression

Searching and filtering output at the --More-- prompt

The --More-- prompt is displayed when output extends beyond a single page. From this prompt, you can press the Space bar to display the next page, the Return or Enter key to display the next line, or Ctrl-C or Q to cancel the display. You can also search and filter output from this prompt.

```
device# ?
  append               Append one file to another
  attrib               Change file attribute
  boot                 Boot system from bootp/tftp server/flash image
  cd                   Change current working directory
  chdir                Change current working directory
  clear                Clear table/statistics/keys
  clock                Set clock
  configure            Enter configuration mode
  copy                 Copy between flash, tftp, config/code
  cp                   Copy file commands
  debug                Enable debugging functions (see also 'undebug')
  delete               Delete file on flash
  dir                  List files
  dm                   test commands
  dot1x                802.1X
  erase                Erase image/configuration files from flash
  exit                 Exit Privileged mode
  fastboot             Select fast-reload option
  force-sync-standby   Sync active flash (pri/sec/mon/startup config/lp images)
                       to standby
  format               Format Auxiliary Flash card
  hd                   Hex dump
  ipc                  IPC commands
--More--, next page: Space, next line: Return key, quit: Control-c
```

At the --More-- prompt, you can press the forward slash key (/) and then enter a search string. The device displays output starting from the first line that contains the search string, similar to the *begin* option for **show** commands.

```
--More--, next page: Space, next line: Return key, quit: Control-c
/telnet
```

The results of the search are displayed.

```
searching...
telnet               Telnet by name or IP address
terminal             Change terminal settings
traceroute           TraceRoute to IP node
undelete             Recover deleted file
whois                WHOIS lookup
write                Write running configuration to flash or terminal
```

To display lines containing only a specified search string (similar to the *include* option for **show** commands) press the plus sign key (+) at the --More-- prompt and then enter the search string.

```
--More--, next page: Space, next line: Return key, quit: Control-c
+telnet
```

The filtered results are displayed.

```
filtering...
  telnet              Telnet by name or IP address
```

To display lines that do not contain a specified search string (similar to the *exclude* option for **show** commands) press the minus sign key (-) at the --More-- prompt and then enter the search string.

```
--More--, next page: Space, next line: Return key, quit: Control-c
-telnet
```

The filtered results are displayed.

```
filtering...
sync-standby         Sync active flash (pri/sec/mon/startup config/lp images)
                     to standby if different
terminal             Change terminal settings
traceroute           TraceRoute to IP node
undelete             Recover deleted file
whois                WHOIS lookup
write                Write running configuration to flash or terminal
```

As with the commands for filtering output from **show** commands, the search string is a regular expression consisting of a single character or string of characters. You can use special characters to construct complex regular expressions. Refer to the next section for information on special characters used with regular expressions.

Using special characters in regular expressions

You can use special characters to construct complex regular expressions to filter output from **show** commands. You can use a regular expression to specify a single character or multiple characters as a search string. In addition, you can include special characters that influence the way the software matches the output against the search string. These special characters are listed in the following table.

TABLE 4 Special characters for regular expressions

Character	Operation
.	The period matches on any single character, including a blank space. For example, the following regular expression matches "aaz", "abz", "acz", and so on, but not just "az": a.z
*	The asterisk matches on zero or more sequential instances of a pattern. For example, the following regular expression matches output that contains the string "abc", followed by zero or more Xs: abcX*
+	The plus sign matches on one or more sequential instances of a pattern. For example, the following regular expression matches output that contains "de", followed by a sequence of "g"s, such as "deg", "degg", "deggg", and so on: deg+
?	The question mark matches on zero occurrences or one occurrence of a pattern. For example, the following regular expression matches output that contains "dg" or "deg": de?g **NOTE** Normally when you type a question mark, the CLI lists the commands or options at that CLI level that begin with the character or string you entered. However, if you enter Ctrl+V and then type a question mark, the question mark is inserted into the command line, allowing you to use it as part of a regular expression.
^	A caret (when not used within brackets) matches on the beginning of an input string.

TABLE 4 Special characters for regular expressions (continued)

Character	Operation
	For example, the following regular expression matches output that begins with "deg": ^deg
$	A dollar sign matches on the end of an input string. For example, the following regular expression matches output that ends with "deg": deg$
_	An underscore matches on one or more of the following: • , (comma) • { (left curly brace) • } (right curly brace) • ((left parenthesis) •) (right parenthesis) • The beginning of the input string • The end of the input string • A blank space For example, the following regular expression matches on "100" but not on "1002", "2100", and so on. _100_
[ ]	Square brackets enclose a range of single-character patterns. For example, the following regular expression matches output that contains "1", "2", "3", "4", or "5": [1-5] You can use the following expression symbols within the brackets. These symbols are allowed only inside the brackets. • ^ - The caret matches on any characters except the ones in the brackets. For example, the following regular expression matches output that does not contain "1", "2", "3", "4", or "5":[^1-5] • - The hyphen separates the beginning and ending of a range of characters. A match occurs if any of the characters within the range is present. See the example above.
|	A vertical bar separates two alternative values or sets of values. The output can match one or the other value. For example, the following regular expression matches output that contains either "abc" or "defg": abc|defg
( )	Parentheses allow you to create complex expressions. For example, the following complex expression matches on "abc", "abcabc", or "defg", but not on "abcdefgdefg": ((abc)+)|((defg)?)

If you want to filter for a special character instead of using the special character as described in the table above, enter "\" (backslash) in front of the character. For example, to filter on output containing an asterisk, enter the asterisk portion of the regular expression as "*".

```
device#show ip route bgp | include \*
```

Allowable characters for LAG names

When creating a LAG name, you can use spaces in a file or subdirectory name if you enclose the name in double quotes. For example, to specify a subdirectory name that contains spaces, enter a string such as the following: "a long subdirectory name". The maximum length for a string is 64 characters.

The following characters are valid in file names:

- All upper and lowercase letters
- All digits

Any of the following special characters are valid:

- $
- %
- '
- -
- _
- .
- @
- ~
- `
- !
- (
-)
- {
- }
- ^
- #
- &

CLI parsing enhancement

The response to an invalid keyword, the command returns to the cursor will include all valid content up to where the error was made. The prompt will only delete the invalid keyword "proc" and return to a prompt with the command "device# **show** ". This will allow the user to continue typing from the point of failure, rather than having to type out the entire command again.

```
device# show proc
Unrecognized command
device# show
```

Syntax shortcuts

A command or parameter can be abbreviated as long as enough text is entered to distinguish it from other commands at that level. For example, given the possible commands **copy tftp** ... and **config tftp** ..., possible shortcuts are **cop tftp** and **con tftp** respectively. In this case, *co* does not properly distinguish the two commands.

Saving configuration changes

You can make configuration changes while the device is running. The type of configuration change determines whether or not it becomes effective immediately or requires a save to flash (**write memory**) and reset of the system (**reload**), before it becomes active.

This approach in adopting configuration changes:

- Allows you to make configuration changes to the operating or running configuration of the device to address a short-term requirement or validate a configuration without overwriting the permanent configuration file, the startup configuration, that is saved in the system flash, and;
- Ensures that dependent or related configuration changes are all cut in at the same time.

In all cases, if you want to make the changes permanent, you need to save the changes to flash using the **write memory** command. When you save the configuration changes to flash, this will become the configuration that is initiated and run at system boot.

> NOTE
> Most configuration changes are dynamic and thus do not require a software reload. If a command requires a software reload to take effect, the documentation states this.

Modifying startup and running configuration file manually

When you manually modify a **startup-config** or **running-config** file, ensure that you do not delete the **! (exclamation mark)** from any of the lines in the configuration file.

> NOTE
> For configuration files which are copied to device running, or startup config via TFTP/SCP, entering a blank comment line or **!** (exclamation mark denotes a comment line) followed only by blank spaces, in any of the global config sublevels, resets the mode to global config level.

Commands A - E

access-list

Defines a numbered access control list (ACL), specifies ACL parameters, and creates the ACL permit and deny rules.

access-list *num* [**permit** | **deny**] [**vlan** *vlan-id*] *ipv6-source-prefix/prefix-length* | *ipv6-source-prefix wildcard-mask* | **any** | **host** *source-ipv6-address ipv6-destination-prefix/prefix-length* | *ipv6-destination-prefix wildcard-mask* | **any** | **host** *ipv6-destination-address* [**ipv6-operator** [*value*]] [**copy-sflow**] | [**drop-precedence** *dp-value*] | [**drop-precedence-force** *dp-value*] | [**dscp** *dscp-value*] | [**dscp-marking** *dscp-value*] [**mirror**] | [**priority-force** *number*] | [**regenerate-seq-num** *dec*] | [**sequence** *number*]

no access-list *num* [**permit** | **deny**] [**vlan** *vlan-id*] *protocol ipv6-source-prefix/prefix-length ipv6-source-prefix wildcard-mask* | **any** | **host** *source-ipv6-address ipv6-destination-prefix/prefix-length* | *ipv6-destination-prefix wildcard-mask* | **any** | **host** *ipv6-destination-address* [**ipv6-operator** [*value*]] [**copy-sflow**] | [**drop-precedence** *dp-value*] | [**drop-precedence-force** *dp-value*] | [**dscp** *dscp_value*] | [**dcsp-marking** *dscp-value*] [**mirror**] | [**priority-force** *number*] | [**regenerate-seq-num** *dec*] | [**sequence** *number*]

No access list is created.

num

Indicates the selected ACL. 1 - 99 are standard IP access list; 100 - 199 are extended IP access lists; 400 -1399 are Level 2 MAC address lists; 2000 - 2999 are UDA access lists.

permit

Indicates that the ACL permits (forwards) packets that match a policy in the ACL.

deny

Indicates that the ACL denies (drops) packets that match a policy in the ACL.

vlan *vlan-id*

Indicates the selected VLAN.

protocol ipv6-source-prefix/prefix-length

Specifies a source or destination prefix and prefix length that a packet must match for the specified deny or permit action to occur. The user must specify the *ipv6-source-prefix* and *ipv6-destination-prefix* parameters in hexadecimal using 16-bit values between colons, as documented in RFC 2373. You must specify the *prefix-length* parameter as a decimal value. A slash (/) must follow the *ipv6-prefix* parameter and precede the *prefix-length* parameter.

ipv6-source-prefix wildcard-mask

Lets the user specify a group of source destination IPv6 addresses. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

any

Specifies instead of the *ipv6-source-prefix/prefix-length* or *ipv6-destination-prefix/prefix-length* parameters matches any IPv6 prefix and is equivalent to the IPv6 prefix ::/0.

host

The **host** *ipv6-source-address* and **host** *ipv6-destination-address* parameter lets you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

source-ipv6-address ipv6-destination-prefix/prefix_length

Specifies a source or destination prefix and prefix length that a packet must match for the specified deny or permit action to occur. The user must specify the *ipv6-source-prefix* and *ipv6-destination-prefix* parameters in hexadecimal

using 16-bit values between colons, as documented in RFC 2373. Th user must specify the *prefix-length* parameter as a decimal value. A slash (/) must follow the *ipv6-prefix* parameter and precede the *prefix-length* parameter.

ipv6-destination-prefix wildcard-mask

Lets you specify a group of host destination IPv6 addresses. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

any

Specifies instead of the *ipv6-source-prefix/prefix-length* or *ipv6-destination-prefix/prefix-length* parameters matches any IPv6 prefix and is equivalent to the IPv6 prefix ::/0.

host

The **host** *ipv6-source-address* and **host** *ipv6-destination-address* parameter lets you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

ipv6-destination-address

Lets you specify a host destination IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

ipv6-operator *value*

If a port has an ACL applied, the user must remove ACL bindings prior to creating or adding that port to a VLAN or a VE interface.

copy-sflow

Sends packets matching the ACL permit clause to the sFlow collector.

drop-precedence *dp-value*

Sets the drop precedence by the selected value.

drop-precedence-force *dp-value*

Sets the force drop precedence by the selected value.

dscp *dscp-value*

Differentiated Services Code Point (DSCP). Enter a value from 0 - 63 for the **dscp** *dscp-value* parameter if you want to filter packets based on their DSCP value.

dscp-marking *dscp-value*

Enter a value from 0 - 64 for the **dscp** *dscp-value* parameter if you want to filter packets based on their DSCP value.

mirror

Mirrors packets matching to the ACL permit clause.

priority-force *number*

Sets the force packet outgoing priority according to the selected number value.

regenerate-seq-num *dec*

Regenerates the filter sequence numbers based on the specified initial resequence number for the access list.

Global configuration mode

You can also create ACLs using the following commands:

- mac access-list—named ACLs
- ip access-list—numbered or named ACLs
- ipv6 access-list—named ACLs

The **no** form of the command removes any definitions to the Access Control List (ACL).

The following example creates a numbered MAC ACL with an ID of 400, defines rules to deny all ARP, IPv6, and MPLS multicast traffic; and permit all other traffic in VLAN 100. The next commands apply that ACL on an ethernet interface to incoming traffic.

```
device# configure terminal
device(config)# access-list 400 deny any any any etype arp
device(config)# access-list 400 deny any any any etype ipv6
device(config)# access-list 400 deny any any any etype 8848
device(config)# access-list 400 permit any any 100

device(config)# interface ethernet 4/12
device(config-int-e100-4/12)# mac access-group 400 in
```

The following example creates a numbered standard IPv4 ACL with an ID of 1, defines rules to deny incoming packets from three source IP addresses; and permit all other traffic. The next commands apply that ACL on an ethernet interface to incoming traffic.

```
device# configure terminal
device(config)# access-list 1 deny host 10.157.22.26
device(config)# access-list 1 deny 10.157.29.12
device(config)# access-list 1 deny host IPHost1
device(config)# access-list 1 permit any

device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group 1 in
```

The following example creates a numbered extended IPv4 ACL with an ID of 101, defines a rule to block all Telnet traffic received from IP host 10.157.22.26; and permit all other traffic. The next commands apply that ACL on an ethernet interface to incoming traffic.

```
device# configure terminal
device(config)# access-list 101 deny tcp host 10.157.22.26 any eq telnet
device(config)# access-list 101 permit ip any any

device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group 1 in
```

Release version	Command history
5.4.00	This command was modified to include the **dscp-marking** *dscp-value* parameter.
5.9.00	This command was modified to include the *ipv6_destination_prefix wildcard-mask* and *pv6-source-prefix wildcard-mask* format to represent a group of addresses. This command was modified to support the UDA ACLs.

access-list (sequence)

Defines a numbered access control list (ACL), specifies ACL parameters, and creates the ACL permit and deny rules. The optional **sequence** keyword enable you to determine the order in which the rules run.

Syntax

access-list *num* [**sequence** *number*] [**permit** | **deny**] [**vlan** *vlan-id*] *protocol ipv6-source-prefix/prefix-length* | *ipv6-source-prefix wildcard-mask* | **any** *hostsource-ipv6_address ipv6-destination-prefix/prefix-length* | *ipv6-destination-prefix wildcard-mask* | **any** | **host** *ipv6-destination-address* [**ipv6-operator** [*value*]] [**copy-sflow**] | [**drop-precedence** *dp-value*] | [**drop-precedence-force** *dp-value*] | [**dscp** *dscp-value*] | [**dscp-marking** *dscp-value*] [**mirror**] | [**priorityforce** *number*] [**match-payload-len**]

no access-list *num* **sequence** *number*] [**permit** | **deny**] [**vlan** *vlan-id*] *protocol ipv6-source-prefix/prefix-length* | *ipv6-source-prefix wildcard-mask* | **any** *hostsource-ipv6_address ipv6-destination-prefix/prefix-length* | *ipv6-destination-prefix wildcard-mask* | **any** | **host** *ipv6-destination-address* [**ipv6-operator** [*value*]] [**copy-sflow**] | [**drop-precedence** *dp-value*] | [**drop-precedence-force** *dp-value*] | [**dscp** *dscp-value*] | [**dscp-marking** *dscp-value*] [**mirror**] | [**priorityforce** *number*] [**match-payload-len**]

Parameters

num

Indicates the selected ACL. 1 - 99 are standard IP access list; 100 - 199 are extended IP access lists; 400 -1399 are Level 2 MAC address lists; 2000 - 2999 are UDA access lists.

sequence *number*

The sequence parameter takes a mandatory decimal integer ranging from 1 to 214748364. When the user tries to use a sequence number that is more than the limit (214748364), it causes the system to generate a sequence number that is greater than the limit. The system generates an error and does not allow the provisioning of the ACL filter.

permit

Indicates that the ACL permits (forwards) packets that match a policy in the ACL.

deny

Indicates that the ACL denies (drops) packets that match a policy in the ACL.

vlan *vlan-id*

Indicates the selected VLAN.

protocol ipv6-source-prefix/prefix-length

Specifies a source or destination prefix and prefix length that a packet must match for the specified deny or permit action to occur. The user must specify the *ipv6-source-prefix* and *ipv6-destination-prefix* parameters in hexadecimal using 16-bit values between colons, as documented in RFC 2373. You must specify the *prefix-length* parameter as a decimal value. A slash (/) must follow the *ipv6-prefix* parameter and precede the *prefix-length* parameter.

ipv6-source-prefix wildcard-mask

Lets the user specify a group source destination IPv6 addresses. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

any

Specifies instead of the *ipv6-source-prefix/prefix-length* or *ipv6-destination-prefix/prefix-length* parameters it matches any IPv6 prefix and is equivalent to the IPv6 prefix ::/0.

host

The **host** *ipv6-source-address* and **host** *ipv6-destination-address* parameter lets you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

source-ipv6-address ipv6-destination-prefix/prefix-length

Specifies a source or destination prefix and prefix length that a packet must match for the specified deny or permit action to occur. The user must specify the *ipv6-source-prefix* and *ipv6-destination-prefix* parameters in hexadecimal using 16-bit values between colons, as documented in RFC 2373. The user must specify the *prefix-length* parameter as a decimal value. A slash (/) must follow the *ipv6-prefix* parameter and precede the *prefix-length* parameter.

ipv6-destination-prefix wildcard-mask

Lets you specify a group of host destination IPv6 addresses. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

any

Specifies instead of the *ipv6-source-prefix/prefix-length* or *ipv6-destination-prefix/prefix-length* parameters it matches any IPv6 prefix and is equivalent to the IPv6 prefix ::/0.

host

The **host** *ipv6-source-address* and **host** *ipv6-destination-address* parameter lets you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

ipv6-destination-address

Lets you specify a host destination IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

ipv6-operator *value*

If a port has an ACL applied, the user must remove ACL bindings prior to creating or adding that port to a VLAN or a VE interface.

copy-sflow

Sends packets matching the ACL permit clause to the sFlow collector.

drop-precedence *dp-value*

Sets the drop precedence by the selected value.

drop-precedence-force *dp-value*

Sets the force drop precedence by the selected value.

dscp *dscp-value*

Enter a value from 0 - 64 for the **dscp** *dscp-value* parameter if you want to filter packets based on their DSCP value.

dscp-marking *dscp-value*

The traffic class bits on all IPv6 packets going to real servers bound to this virtual server are set to the configured value. The dscp-marking value ranges from 0 - 64.

mirror

Mirror packets matching the ACL permit clause.

priorityforce *number*

Sets the force packet outgoing priority according to the selected number value.

Modes

Global configuration mode.

Usage Guidelines

You can also create ACLs using the following commands:

- mac access-list—named ACLs
- ip access-list—numbered or named ACLs
- ipv6 access-list—named ACLs

The **no** form of the command removed the definitions from the *Access Control List (ACL).*

Examples

The following example creates a numbered MAC ACL with an ID of 400, defines sequential rules to deny all ARP, IPv6, and MPLS multicast traffic; and permit all other traffic in VLAN 100. The next commands apply that ACL on an ethernet interface to incoming traffic.

```
device# configure terminal
device(config)# access-list 400 sequence 10 deny any any any etype arp
device(config)# access-list 400 sequence 10 deny any any any etype ipv6
device(config)# access-list 400 sequence 10 deny any any any etype 8848
device(config)# access-list 400 sequence 10 permit any any 100

device(config)# interface ethernet 4/12
device(config-int-e100-4/12)# mac access-group 400 in
```

The following example creates a numbered standard IPv4 ACL with an ID of 1, defines sequential rules to deny incoming packets from three source IP addresses; and permit all other traffic. The next commands apply that ACL on an ethernet interface to incoming traffic.

```
device# configure terminal
device(config)# access-list 1 sequence 100 deny host 10.157.22.26
device(config)# access-list 1 sequence 200 deny 10.157.29.12
device(config)# access-list 1 sequence 300 deny host IPHost1
device(config)# access-list 1 sequence 400 permit any
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group 1 in
```

The following example creates a numbered extended IPv4 ACL with an ID of 102, and defines sequential rules to:

- Permit ICMP traffic from hosts in the 10.157.22.x network to hosts in the 10.157.21.x network.
- Deny IGMP traffic from the host "rkwong" device to the 10.157.21.x network.
- Deny IGRP traffic from the 10.157.21.x network to the "rkwong" device.
- Deny all IP traffic from host 10.157.21.100 to host 10.157.22.1.
- Deny all OSPF traffic.
- Permit all other traffic.

The next commands apply that ACL on one port to incoming traffic and on another port to outgoing traffic.

```
device# configure terminal
device(config)# access-list 102 sequence 110 permit icmp 10.157.22.0/24 10.157.21.0/24
device(config)# access-list 102 sequence 120 deny igmp host rkwong 10.157.21.0/24
device(config)# access-list 102 sequence 130 deny igrp 10.157.21.0/24 host rkwong
device(config)# access-list 102 sequence 140 deny ip host 10.157.21.100 host 10.157.22.1
device(config)# access-list 102 sequence 150 deny ospf any any
device(config)# access-list 102 sequence 160 permit ip any any

device(config)# interface ethernet 1/2
device(config-if-e10000-1/2)# ip access-group 102 in
device(config-if-e10000-1/2)# exit
device(config)# interface ethernet 4/3
device(config-if-e10000-4/3)# ip access-group 102 out
```

History

Release version	Command history
5.9.00	This command was modified to include the *ipv6-source-prefix wildcard-mask* and *ipv6-destination-prefix wildcard-mask* format to represent a group of addresses.

activate (VRRP)

Activates the configured Virtual Router Redundancy Protocol (VRRP) virtual routing instance.

Syntax

activate

no activate

Command Default

A VRRP virtual routing instance is not activated.

Modes

VRID interface configuration mode

Usage Guidelines

Before issuing this command, complete the configuration of the VRRP virtual router. The interface assigned to the Virtual Routing ID (VRID) does not provide backup service for the virtual IP address until you activate the VRRP configuration.

The **no** form of this command disables the VRRP VRID.

Examples

The following example configures and activates VRRP VRID 1.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
VRRP router 1 for this interface is activating
```

activate (VSRP)

Activates the Virtual Switch Redundancy Protocol (VSRP) Virtual Router ID (VRID) for a port-based VLAN.

Syntax

activate

no activate

Command Default

The VRID is not activated by default.

Modes

VSRP VRID configuration mode

Usage Guidelines

The device must be set as a backup. Because VSRP does not have an owner, all VSRP devices are backups. The active device for a VRID is elected based on the VRID priority, which is configurable.

The **no** form of the command deactivates the VSRP VRID on the VLAN.

Examples

The following example shows how to activate the VSRP on a VLAN.

```
device(config)# vlan 200
device(config-vlan-200)# tag ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# backup
device(config-vlan-200-vrid-1)# activate
```

additional-paths

Enables additional paths capability for all BGP neighbors under the configured address family.

Syntax

additional-paths receive [**send**]

additional-paths send [**receive**]

no additional-paths receive [**send**]

no additional-paths send [**receive**]

Command Default

Additional paths are not advertised.

Parameters

receive

Enables BGP capability to receive additional paths from BGP neighbors.

send

Enables BGP capability to send additional paths to BGP neighbors.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 multicast configuration mode

BGP address-family IPv6 multicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Capability configured at the peer level using the **neighbor additional-paths** command or at peer-group level overrides any send or receive capability configured using this command.

The **no** form of the command disables the advertisement of additional paths for BGP neighbors under the configured address family.

Examples

The following example enables BGP4 capability to send additional paths to BGP neighbors and receive additional paths from BGP neighbors under the IPv4 unicast address family.

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

The following example enables BGP4+ capability to receive additional paths from all BGP neighbors under the IPv6 unicast address family.

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

History

Release version	Command history
6.0.0	This command was introduced.

additional-paths select

Selects paths as candidates for additional paths under the configured address family.

Syntax

additional-paths select all [**best** *number*] [**group-best**]

additional-paths select best *number* [**all**] [**group-best**]

additional-paths select group-best [**all**] [**best** *number*]

no additional-paths select { **all** | **best** *number* | **group-best** }

Command Default

Paths are not selected.

Parameters

all

Specifies that all paths are eligible to be selected. The maximum number of paths is 16.

best

The paths that the device selects as best paths are selected.

number

Specifies the number of best paths selected. Valid values range from 2 through 16.

group-best

Specifies that all the group best paths are eligible for selection. If the rank of any group-best add-path is more than 16, its is not advertised.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 multicast configuration mode

BGP address-family IPv6 multicast 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 specified candidate from the filter list.

Examples

The following example specifies that all BGP paths are eligible to be selected as additional paths under the IPv4 unicast address family.

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

The following example specifies that the nine best BGP paths are eligible to be selected as additional paths under the IPv6 multicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 multicast
device(config-bgp-ipv6m)# additional-paths select best 9
```

The following example specifies that the group best BGP paths are eligible to be selected as additional paths under the IPv6 unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 multicast
device(config-bgp-ipv6u)# additional-paths select group-best
```

History

Release version	Command history
6.0.0	This command was introduced.

address-family multicast (BGP)

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

Syntax

address-family ipv4 multicast

address-family ipv6 multicast

no address-family ipv4 multicast

no address-family ipv6 multicast

Parameters

ipv4

Specifies an IPv4 address family.

ipv6

Specifies an IPv6 address family.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

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

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 multicast
device(config-bgp-ipv4m)#
```

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

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 multicast
device(config-bgp-ipv6m)#
```

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 unicast [**vrf** *vrf-name*]

address-family ipv6 unicast [**vrf** *vrf-name*]

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

no address-family 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

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

Examples

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

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

The following example enables BGP IPv4 address family unicast configuration mode for VRF “green”.

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

address-family unicast (IS-IS)

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

Syntax

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

Command Default

Disabled.

Parameters

ipv4

Specifies the IPv4 address family.

ipv6

Specifies the IPv6 address family.

Modes

IS-IS router configuration mode

Examples

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

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

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

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

adjacency-check

Enables IS-IS IPv6 protocol-support consistency checks that are performed prior to forming adjacencies on hello packets.

Syntax

adjacency-check

no adjacency-check

Command Default

Enabled.

Modes

ISIS address-family IPv6 unicast configuration mode

Usage Guidelines

The **no** form of the command disables the IS-IS IPv6 protocol-support consistency checks.

Examples

The following example disables the IS-IS IPv6 protocol-support consistency checks.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# no adjacency-check
```

The following example re-enables the IS-IS IPv6 protocol-support consistency checks.

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

adjustment-threshold

Specifies the sensitivity of the automatic bandwidth adjustment of a label-switched path (LSP) to changes in bandwidth utilization.

Syntax

adjustment-threshold [*num* | **use-threshold-table**]

no adjustment-threshold [*num* | **use-threshold-table**]

Parameters

num

Defines the adjustment threshold in percent. The range is 0 - 100. The default is 0.

use-threshold-table

Indicates that the template has to use the autobw-threshold table to determine the threshold.

Modes

MPLS auto-bandwidth template configuration mode.

MPLS LSP auto-bandwidth configuration mode.

Usage Guidelines

Under the MPLS auto-template configuration mode, the command sets the threshold for when to trigger automatic bandwidth adjustments. When the automatic bandwidth adjustment is configured, bandwidth demand for the current interval is determined and compared to the LSPs current bandwidth allocation.

Under the MPLS LSP autobw configuration mode, the command configures the LSP path to use adjustment-threshold from the autobw-threshold table instead of a percentage.

Under both configuration modes, the **no** form of the command sets the adjustment threshold to the default value.

Examples

The following example under the MPLS autobw-template config mode configures the automatic bandwidth adjustment template to use the autobw-threshold table to determine the threshold.

```
deviceconfig terminal
device(config)# router mpls
device(config-mpls)# autobw-template template1
device(config-mpls-autobw-template-template1)# adjustment-interval 1200
device(config-mpls-autobw-template-template1)# adjustment-threshold use-threshold-table
device(config-mpls-autobw-template-template1)# overflow-limit 10
device(config-mpls-autobw-template-template1)# underflow-limit 20
device(config-mpls-autobw-template-template1)# sample-recording enable
```

The following example under the MPLS lsp autobw config mode defines the automatic bandwidth adjustment threshold as 40 percent.

```
deviceconfig terminal
device(config)# router mpls
device(config-mpls)# lsp lsp1
device(config-mpls-lsp-lsp1)# adaptive
device(config-mpls-lsp-lsp1)# auto-bandwidth
device(config-mpls-lsp-lsp1-autobw)# template template1
device(config-mpls-lsp-lsp1-autobw-template-template1)# overflow-limit 0
device(config-mpls-lsp-lsp1-autobw-template-template1)# underflow-limit 20
device(config-mpls-lsp-lsp1-autobw-template-template1)# mode monitor-only
device(config-mpls-lsp-lsp1-autobw-template-template1)# sample-recording disable
```

History

Release	Command history
5.6.00	The command was introduced.

advertise backup

Advertises a Virtual Router Redundancy Protocol (VRRP) backup router to a VRRP master router.

Syntax

advertise backup

no advertise backup

Command Default

A VRRP backup router does not advertise itself to a VRRP master router.

Modes

VRID interface configuration mode

Usage Guidelines

Hello messages are used to advertise a backup router to a master router. To configure the interval at which the messages are sent, use the **backup-hello-interval** command.

The **advertise backup** command is configured only on VRRP backup routers and is supported by VRRP and VRRP-E.

The **no** form of the command disables the advertisement of a VRRP backup router to a VRRP master router.

Examples

The following example enables advertisements from the VRRP backup router and configures the hello message interval to 10 seconds.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# advertise backup
device(config-if-e1000-1/6-vrid-1)# backup-hello-interval 10
```

advertise backup (vsrp)

Enables a backup to send Hello messages to the master.

Syntax

advertise backup

no advertise backup

Command Default

By default, backups do not send Hello messages to advertise themselves to the master.

Modes

VSRP VRID configuration mode

Usage Guidelines

When a backup is enabled to send Hello messages, the backup sends a Hello message to the master every 600 units of 100 milliseconds by default. You can change the interval to be from 600 - 3600 units of 100 milliseconds using the **backup-hello-interval** command.

The **no** form of the command disables the backup from sending the Hello messages.

Examples

The following example enables a backup to send Hello messages to the master.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vsrp-1)# backup
device(config-vlan-200-vsrp-1)# advertise backup
```

advertise-best-external

Enables BGP to advertise the best external route to its IBGP neighbors even when it is not the best route.

Syntax

advertise-best-external

no advertise-best-external

Command Default

The best external path is not calculated.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 multicast configuration mode

BGP address-family IPv6 multicast 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 advertising of the best external route under the configured address family.

Examples

The following example enables BGP4+ to advertise the best external route to its neighbors.

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

History

Release version	Command history
6.0.0	This command was introduced.

advertise-fec

Configures the prefix-list to inject the routes learned by routing into the LDP and advertises the FEC to other LDP peers.

Syntax

advertise-fec *prefix-list*

no advertise-fec *prefix-list*

Parameters

prefix-list

The prefix-list specifies the prefixes. The range is an ASCII string, which is the Prefix List Name.

Modes

MPLS LDP configuration mode.

Usage Guidelines

Use to configure the prefix-list to inject the routes learned by routing into the LDP and advertises the FEC to other LDP peers. This command is similar to the **filter-fec** command used for inbound and outbound FEC filtering in LDP. This command is mutually exclusive with the ACL based command (advertise-labels), and only one of the two configurations can be present at any given time. When the ACL based configuration is already present, an error message displays to the operator to un-configure the ACL in LDP and the prefix-list command is rejected.

The command syntax is similar to the **filter-fec** command used for inbound and outbound FEC filtering in LDP.

The **no** form of the command removes the prefix listing.

Examples

The following example displays the prefix-list when no ACL configuration is in the LDP:

```
device(config)# ip prefix-list list-abc deny 44.44.44.44/32
device(config)# ip prefix-list list-abc permit 0.0.0.0/0 ge 32

device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# advertise-fec list-abc
```

History

Release version	Command history
5.7.00	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 address aggregation feature is disabled. By default, the device advertises individual routes for all networks.

Parameters

ip-addr
IPv4 address.

ip-mask
IPv4 mask.

ipv6-addr
IPv6 address.

ipv6-mask
IPv6 mask.

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

map-name
Specifies a route map to be consulted.

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 multicast configuration mode

BGP address-family IPv6 multicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Examples

This example aggregates routes from a range of networks into a single network prefix under the IPv4 address family and advertises the paths for this route as AS_SET.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# aggregate-address 10.1.1.1/8 as-set
```

This example aggregates routes from a range of networks into a single network prefix for BGP VRF instance "red":

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# aggregate-address 5.0.0.0/8
```

This example aggregates routes from a range of networks into a single network prefix prevents the device from advertising more-specific routes under the IPv6 multicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u)# aggregate-address 2001:db8::12d:1300/64 summary-only
```

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

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

This example configures the device always to compare the MEDs.

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

area authentication

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

Syntax

area { *ip-address* | *decimal* } **authentication ipsec spi** *value* **esp sha1** *key*

area { *ip-address* | *decimal* } **authentication ipsec spi** *value* **esp sha1 no-encrypt** *key*

no area { *ipv6-address* | *decimal* } **authentication ipsec spi** *value*

Command Default

Authentication is not enabled on an area.

The key is stored in encrypted format by default.

Parameters

ip-address

Area ID in IP address format.

decimal

Area ID in decimal format.

ipsec

Specifies that IP security (IPsec) is the protocol that authenticates the packets.

spi

Specifies the Security Policy Index (SPI).

value

Specifies the SPI value. Valid values range from decimal numbers 256 through 4294967295. The near-end and far-end values must be the same.

esp

Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security. This is the only option currently available.

sha1

Enables Hashed Message Authentication Code (HMAC) Secure Hash Algorithm 1 (SHA-1) authentication on the OSPFv3 area.

key

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

no-encrypt

The 40-character key is not encrypted upon either its entry or its display.

key

The 40 hexadecimal character key.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The 40 hexadecimal character key is encrypted by default. The system adds the following in the configuration to indicate that the key is encrypted:

- encrypt = the key string uses proprietary simple cryptographic 2-way algorithm (only for Brocade NetIron CES and Brocade NetIron CER devices)
- encryptb64 = the key string uses proprietary base64 cryptographic 2-way algorithm (only for Brocade NetIron XMR and Brocade MLX series devices)

Use the **no-encrypt** parameter to disable encryption.

Currently certain keyword parameters must be entered though only one keyword choice is possible for that parameter. For example, the only authentication algorithm is HMAC-SHA1-96, but you must nevertheless enter the **sha1** keyword for this algorithm. Also, although ESP is currently the only authentication protocol, you must enter the **esp** keyword.

The **no** form of the command removes an authentication specification for an area from the configuration.

Examples

The following example enables esp and SHA-1 authentication for an OSPFv3 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-ospf6-router)# area 0 authentication ipsec spi 750 esp sha1
abcef12345678901234fedcba098765432109876
```

area nssa (OSPFv2)

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

Syntax

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

area { *ip-addr* | *decimal* } **nssa default-information-metric** { *num* | **metric-type** { **type1** | **type2** } }

area { *ip-addr* | *decimal* } **nssa default-information-originate**

area { *ip-addr* | *decimal* } **nssa no-redistribution**

area { *ip-addr* | *decimal* } **nssa translator-always**

area { *ip-addr* | *decimal* } **nssa 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 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 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.

default-information-metric *metric*

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. Valid values range from 1 through 16777215.

metric-type *num*

Specifies how the cost of a neighbor metric is determined. The default is type2.

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.

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.

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.

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 device.Valid values range from 10 through 60 seconds.

Modes

OSPFv2 router configuration mode

OSPFv2 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)# router ospf
device(config-ospf-router)# area 8 nssa 4 no-summary
```

area nssa (OSPFv3)

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

Syntax

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

no area nssa

Command Default

No areas are created.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

metric

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

default-information-originate

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

metric-type

Specifies how the cost of a neighbor metric is determined.

type1

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

type2

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

no-redistribution

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

no-summary

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

translator-always

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

translator-interval *interval*

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

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

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

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

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

Examples

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

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# area 8 nssa 4 no-summary
```

area prefix-list (OSPFv2)

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

Syntax

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

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

Command Default

Disabled.

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

prefix-list *name*
Specifies a prefix-list.

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-ospf-router)# 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-ospf-router)# area 10.1.1.1 prefix-list myprefixlist in
```

area range (OSPFv2)

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

Syntax

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

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* **cost** *cost_value*

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

no area range

Command Default

The address range is advertised.

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-ospf-router)# area 3 range 10.1.1.0 10.255.255.0 advertise
```

area range (OSPFv3)

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

Syntax

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

no area range

Parameters

ip-addr
Area address in IP address format.

decimal
Area address in decimal format.

ipv6 address/mask
Specifies the IPv6 address in dotted-decimal notation and the IPv6 mask in CIDR notation. All network addresses that match this network are summarized in a single route and advertised by the ABR.

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

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

not-advertise
Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting is used to temporarily pause route summarization from the area.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

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

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

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

Examples

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

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# area 3 range 2001:db8:8::/45 advertise
```

area stub (OSPFv2)

Creates or deletes a stub area or modifies its parameters.

Syntax

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

no area stub

Command Default

No areas are created.

Parameters

A.B.C.D

Area address in IP address format.

decimal

Area address In decimal format.

metric

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

no-summary

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

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

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

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

Examples

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

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

area stub (OSPFv3)

Creates or deletes a stub area or modifies its parameters.

Syntax

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

no area stub

Command Default

No areas are created.

Parameters

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-ospf6-router)# area 2 stub 5
```

area virtual-link (OSPFv2)

Creates or modifies virtual links for an area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *E.F.G.H* [**authentication-key** { **0** | **1** | **2** } *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

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.

0

Does not encrypt the password you enter.

1

The key string uses proprietary simple cryptographic 2-way algorithm.

2

The key string uses proprietary base64 cryptographic 2-way algorithm (only for Brocade NetIron XMR and Brocade NetIron MLX Series devices).

password

OSPF password. The password can be up to eight alphanumeric characters.

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 2147483647 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-ospf-router)# area 1 virtual-link 10.1.2.3
```

area virtual-link (OSPFv3)

Creates or modifies virtual links for an area.

Syntax

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

no area virtual-link

Command Default

No virtual links are created.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

A.B.C.D

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

dead-interval *time*

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

hello-interval *time*

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

hello-jitter *interval*

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

retransmit-interval *time*

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

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-ospf6-router)# area 1 virtual-link 209.157.22.1
```

area virtual-link authentication (OSPFv3)

Enables authentication for virtual links in an OSPFv3 area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *E.F.G.H* **authentication ipsec spi** *value* **esp sha1** *key* [**no-encrypt**] *key*

no area { *IPv6 address* | *decimal* } **virtual-link** *E.F.G.H* **authentication ipsec spi** *spi*

Command Default

Authentication is not enabled on a virtual-link.

The 40 hexadecimal character key is encrypted by default. Use the **no-encrypt** parameter to disable encryption.

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.

ipsec

Specifies that IP security (IPsec) is the protocol that authenticates the packets.

spi

Specifies the Security Policy Index (SPI).

value

Specifies the SPI value. Valid values range from decimal numbers 256 through 4294967295. The near-end and far-end values must be the same.

esp

Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security. This is the only option currently available.

sha1

Enables Hashed Message Authentication Code (HMAC) Secure Hash Algorithm 1 (SHA-1) authentication on the OSPFv3 area.

key

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

no-encrypt

The 40-character key is not encrypted upon either its entry or its display.

key

The 40 hexadecimal character key.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Currently certain keyword parameters must be entered though only one keyword choice is possible for that parameter. For example, the only authentication algorithm is HMAC-SHA1-96, but you must nevertheless enter the **sha1** keyword for this algorithm. Also, although ESP is currently the only authentication protocol, you must enter the **esp** keyword.

The **no** form of the command removes authentication from the virtual-links in the area.

Examples

The following example configures IPsec on a virtual link in an OSPFv3 area, and encryption is disabled.

```
device# configure terminal
device(config)# ip router-id 10.1.2.2
device(config)# ipv6 router ospf
device(config-ospf6-router)# area 2 virtual-link 10.1.2.2 authentication ipsec spi 600 esp sha1 no-
encrypt 1134567890223456789012345678901234567890
```

arp

Correlates an IP address and a Media Access Control (MAC) address for a device on the network to form a static ARP entry. Static ARP entries do not age out of the ARP table.

Syntax

arp *ip_addr mac_addr* [**ethernet** *slot/port* | **vlan** *vlan_id*]

no arp *ip_addr mac_addr* [**ethernet** *slot/port* | **vlan** *vlan_id*]

arp *ip_addr mac_addr* [**multi-ports** { **ethernet** *slot/port* [**ethernet** *slot/port . . .*] | **ethernet** *slot/port* **to** *slot/port* } | { **pos** *slot/port* [**pos** *slot/port . . .*] | **pos** *slot/port* **to** *slot/port* }]

no arp *ip_addr mac_addr* [**multi-ports** { **ethernet** *slot/port* [**ethernet** *slot/port . . .*] | **ethernet** *slot/port* **to** *slot/port* } | { **pos** *slot/port* [**pos** *slot/port . . .*] | **pos** *slot/port* **to** *slot/port* }]

arp *ip_addr mac_addr* [**multi-ports** { **ethernet** *slot/port* **ethernet** *slot/port* **ethernet** *slot/port* | **ethernet** *slot/port* **to** *slot/port* } | { **pos** *slot/port* **pos** *slot/port* **pos** *slot/port* | *slot/port* **to** *slot/port* }]

no arp *ip_addr mac_addr* [**multi-ports** { **ethernet** *slot/port* **ethernet** *slot/port* **ethernet** *slot/port* | **ethernet** *slot/port* **to** *slot/port* } | { **pos** *slot/port* **pos** *slot/port* **pos** *slot/port* | *slot/port* **to** *slot/port* }]

arp *ip_addr mac_addr* [**vpls** { **peer** *ip_addr* | **vlan** *vlan_id* **ethernet** *slot/port* }]

no arp *ip_addr mac_addr* [**vpls** { **peer** *ip_addr* | **vlan** *vlan_id* **ethernet** *slot/port* }]

Parameters

ip_addr
: Specifies the IPv4 address of the host.

mac_addr
: Specifies the MAC address of the host. The MAC address must be entered in the hexadecimal format.

ethernet *slot/port*
: Specifies the selected Ethernet port.

multi-ports
: Configures multi-ports static ARP. See "Usage Guidelines."

  ethernet
  : Configures the static ARP entry on the Ethernet port.

  pos
  : Configures the static ARP entry on the POS port.

vlan *vlan_id*
: Configures static ARP entry for a VLAN. The VLAN ID range is from 1 to 4090.

vpls
: Configures static ARP entry for a VPLS instance.

  peer
  : Configures the VPLS-peer IP address.

vlan

Configures the VLAN ID.

Modes

Global configuration mode.

VRF sub-configuration mode.

Usage Guidelines

Use the **no** form of the command to remove a static mapping address.

If the VLAN ID is not configured when IP source guard is turned on, the IP address is assumed to be valid on all the VLANS on the port.

If both the VLAN ID and the port are not configured when IP source guard is turned on, the IP address is assumed to be valid for all VLANs.

The multi-ports option allows you to assign multiple ports in the same VE to a single static ARP entry. The option can be used in a pure Layer 3 forwarding environment to forward IPv4 traffic from multiple ports but should not be used in conjunction with multiport static MAC. When you use the multi-ports option, you can create a list of interfaces, a range of interfaces, or a combination. You can use multiple lists and ranges in the same command line.

Examples

The following example creates a basic static ARP entry for IP address 10.1.1.1 and MAC address 0001.0002.0003.

```
device# configure terminal
device(config)# arp 10.1.1.1 0001.0002.0003
```

The following example creates a static ARP entry for multiple ports, including a list of ports (1/1, 2/1, and 2/3), two port ranges (3/3 to 3/6 and 4/3 to 4/8), and a final list of ports (5/1, 5/6, 5/7).

```
device# configure terminal
device(config)# arp 10.2.5.4 1001.2002.3003 multi-ports ethernet 1/1 ethernet 2/1 ethernet 2/3 ethernet
3/3 to 3/6 ethernet 4/3 to 4/8
ethernet 5/1 ethernet 5/6 ehternet 5/7
```

The following example shows an ARP configuration command for a VRF that is extended to support VPLS instances.

```
device# configure terminal
device(config)# vrf red
device(config-vrf-red# rd 55:55
device(config-vrf-red)address-family ipv4
device(config-vrf-red-ipv4)# arp 10.1.1.1 0001.0002.0003  vpls vlan 10 ethernet 1/1
```

History

Release version	Command history
5.8.00	This command was modified to enable VRF for VPLS VE.

arp-guard

Discards all gratuitous ARP and ARP replies for IP addresses not permitted by the specified ARP-guard standard IP access control list (ACL).

Syntax

arp-guard *arp-guard-access-list-name*

no arp-guard *arp-guard-access-list-name*

Command Default

All gratuitous ARP and ARP replies for IP addresses are software forwarded.

Parameters

arp-guard-access-list-name

ARP packets that do not match the specified ARP guard ACL are dropped by the LP and those which match will be software forwarded.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command removes the ARP-guard filtering of ARP packets.

This command is used in conjunction with the **arp-guard-access-list** command to build a table of allowed IP addresses on the link on which the ARP-guard feature is enabled.

Examples

The following example configures the ARP-guard feature to discard all gratuitous ARP and ARP replies for IP addresses that do not match the IP address and MAC address listed in the ACL named arpacl10.

```
device# configure terminal
device(config)# interface ethernet 1/6
device(conf-if-e1000-1/6)# arp-guard-access-list AS201
device(conf-if-e1000-1/6)# permit 10.0.0.2  0001.0002.0003
device(conf-if-e1000-1/6)# arp-guard arpacl10
```

History

Release version	Command history
5.7.00	This command was introduced.

arp-guard-access-list

Creates the ARP guard access list.

Syntax

arp-guard-access-list *arp-guard-access-list-name*

no arp-guard-access-list *arp-guard-access-list-name*

Command Default

No ARP guard access list is created.

Parameters

arp-guard-access-list-name

The name of the ARP guard access-list, which contains the list of rules and filters for a specific ARP ACL.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command removes the ARP guard group.

Examples

The following example creates an ARP guard access list named AS201.

```
device# configure terminal
device(config)# arp-guard-access-list AS201
```

History

Release version	Command history
5.7.00	This command is introduced.

arp-guard-syslog-timer

Sets the system log timer duration for an ARP guard.

Syntax

arp-guard-syslog-timer *dec*

no arp-guard-syslog-timer *dec*

Command Default

By default, ARP guard syslog messages for the dropped packets are displayed on the active console for every 60 seconds.

Parameters

dec	The syslog timer duration that is configurable in seconds. The default value is 60 seconds.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command removes the syslog timer value.

Examples

The following command example is used to set the system log timer value at 240 seconds.

```
Brocade(config)# arp-guard-syslog-timer 240
Brocade(config)# show arp-guard-access-list all
Arp-guard configuration:
!
arp-guard-access-list AS200
!
arp-guard-access-list AS201
permit  any 1.1.1.1 any
permit  any 1.1.1.1 0001.0001.0001
!
arp-guard-syslog-timer 240
!
```

History

Release version	Command history
5.7.00	This command is 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

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

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

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

authentication (IKEv2)

Configures an authentication proposal for an Internet Key Exchange version 2 (IKEv2) profile.

Syntax

authentication *authentication-proposal-name*

Parameters

authentication-proposal-name

Specifies the name of an authentication proposal.

Modes

IKEv2 profile configuration mode

Examples

The following example shows how to configure an authentication proposal named auth_test1 for an IKEv2 profile named ikev2_profile.

```
device# configure terminal
device(config)# ikev2 profile ikev2_profile
device(config-ikev2-profile-ikev2_profile)# authentication auth_test1
```

History

Release version	Command history
5.8.00	This command was introduced.

auth-check

Enables Intermediate System-to-Intermediate System (IS-IS) authentication checking.

Syntax

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

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

Command Default

IS-IS authentication checking is enabled by default.

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

ISIS router configuration mode

Usage Guidelines

The **no** form of the command disables IS-IS authentication checking.

Examples

The following example re-enables IS-IS authentication checking for Level 1 packets if it has been disabled.

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

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

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no auth-check level-2
```

auth-key

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

Syntax

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

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

Command Default

No authentication key is configured.

Parameters

string

Specifies a text string that is used as an authentication password.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

ISIS router configuration mode

Usage Guidelines

By default, the authentication key is encrypted. If you want the authentication key to be in clear text, insert a **0** between **auth-key** and *string*.

The authentication mode must be configured using the **auth-mode** command before a *string* can be configured. If the authentication mode is reset for the level specified, the authentication key must also be reset.

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

Examples

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

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-key 0 mysecurekey level-1
```

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

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

auth-mode

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

Syntax

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

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

Command Default

Disabled.

Parameters

cleartext

Specifies clear text authentication.

md5

Specifies message Digest 5 (MD5) authentication.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

ISIS router configuration mode

Usage Guidelines

The **no** form of the command removes the configured authentication mode.

Examples

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

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-mode MD5 level-1
```

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

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

auto-bandwidth

Allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel.

Syntax

auto-bandwidth sample-interval *sec*

no auto-bandwidth sample-interval *sec*

Parameters

sample-interval *sec*

The **sample-interval** parameter is the time after which the traffic rate is sampled. The *sec* variable sets the sample interval in seconds. Range is 60 - 604,800 (7 days). Default is 300 seconds.

Modes

Global configuration mode.

MPLS configuration mode (config-mpls-policy).

Usage Guidelines

The **no** function disables the auto-bandwidth globally. Auto-bandwidth suspends functionality like the adjustment of bandwidth, rate-calculation, and timers. The rates for the auto-bandwidth LSP revert to traffic-engineering configured mean-rate.

The **auto-bandwidth sample-interval** *sec* command enables global auto-bandwidth and sets sample-interval to the entered value.

The **no auto-bandwidth** command disables global auto-bandwidth without changing the sample-interval.

NOTE
Disabling auto-bandwidth globally does not revert to the configured sample-interval value.

Examples

The following example displays the **auto-bandwidth** command that enables auto-bandwidth globally:

```
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# auto-bandwidth sample-interval 30
```

The following example displays the command to enter the auto-bandwidth mode of the CLI for the primary/secondary path.

```
device(config-mpls-lsp-xyz)# auto-bandwidth         (for primary path)
device(config-mpls-lsp-xyz-secpath-xyz2)# auto-bandwidth     (for secondary path)
```

History

Release version	Command history
5.3.00	This command was introduced.

autobw-threshold-table

Configures the MPLS auto-bandwidth threshold table.

Syntax

autobw-threshold-table

no autobw-threshold table

Modes

MPLS configuration mode.

MPLS auto-bandwidth threshold table configuration mode.

MPLS LSP configuration mode.

Usage Guidelines

The **no** form of the command clears all the entries in the adjustment-threshold table.

Examples

The following example shows when the user wants to set the adjustment-threshold table.

```
device(config)# router mpls
device(config-mpls)# autobw-threshold-table
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 10 threshold 2000
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 1000 threshold 3000
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 10000 threshold 5000
```

The following example shows when the user wants to remove one of the threshold entries.

```
device(config)# router mpls
device(config-mpls)# autobw-threshold-table
device(config-mpls-autobw-threshold-table)# no bandwidth-ceiling 1000 threshold 3000
```

The following example shows when the user wants to clear the threshold table.

```
device(config)# router mpls
device(config-mpls)# no autobw-threshold-table
```

The following example shows when the user wants to configure an LSP to use the global table for adjustment threshold.

```
device(config)# router mpls
device(config-mpls)# lsp lsp1
device(config-mpls-lsp-lsp1)# auto
device(config-mpls-lsp-lsp1-autobw)# adjustment-threshold use-threshold-table
```

History

Release	Command history
5.6.00	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

Command Default

Reference bandwidth is 100 Mbps.

Parameters

value

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

use-active-ports

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

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

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

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

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The 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-ospf-router)# auto-cost reference-bandwidth 500
```

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

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.

The costs for 10 Mbps and 100 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

auto-cost reference-bandwidth (OSPFv3)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth *value*

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

value

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

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use this command to configure the cost of an interface that a device advertises to it's OSPF neighbors. OSPFv3 calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

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

- LAG group — The combined bandwidth of all the ports.
- Virtual (Ethernet) 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.

Some interface types are not affected by the reference bandwidth and always have the same cost regardless of the reference bandwidth in use:

- The cost of a loopback interface is always 1.
- The cost of a virtual link is calculated using the Shortest Path First (SPF) algorithm and is not affected by the auto-cost feature.
- The bandwidth for tunnel interfaces is 9 Kbps and is subject to the auto-cost feature.

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-ospf6-router)# auto-cost reference-bandwidth 500
```

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

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.
- 155 Mbps port cost = 500/155 = 3.23, which is rounded up to 4
- 622 Mbps port cost = 500/622 = 0.80, which is rounded up to 1
- 2488 Mbps port cost = 500/2488 = 0.20, which is rounded up to 1

The costs for 10 Mbps, 100 Mbps, and 155 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

auto-enroll

Sends enrollment messages to the certificate authority (CA) and local certificates to either generate new key pair for a certificate or renew an expired certificate.

Syntax

auto-enroll [**regenerate** | *percent*]

no auto-enroll [**regenerate** | *percent*]

Command Default

The option to send enrollment messages is disabled.

Parameters

regenerate

Generates a new key pair for the certificate even if the key pair already exists.

percent

Specifies the renewal percentage value to request a new certificate. Valid percentage values range from 10 through 90 percent. The default is 80 percent.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The **no** form of the command disables the device from sending enrollment messages.

Examples

The following example specifies the percentage value as 20.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# auto-enroll 20
```

The following example specifies the option of regenerating a new key pair for a certificate.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# auto-enroll regenerate
```

History

Release version	Command history
5.9.00	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

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

The **auto-shutdown-new-neighbors** command applies to all neighbors configured under each VRF. When the **auto-shutdown-new-neighbors** command is used, any new neighbor configured will have the shutdown flag enabled for them by default. Once all the neighbor parameters are configured and it is ready to start the establishment of BGP session with the remote peer, the BGP neighbor's shutdown parameter has to disabled by removing the shutdown command for the neighbor.

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

Examples

The following example enables auto shutdown of BGP neighbors on initial configuration.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# auto-shutdown-new-neighbors
```

backup

Designates a virtual router as a Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) backup device and configures priority and track values.

Syntax

backup [**priority** *value*] [**track-priority** *value*]

no backup [**priority** *value*] [**track-priority** *value*]

Command Default

No virtual routers are designated as a VRRP or VRRP-E backup device.

Parameters

priority *value*

Sets a priority value for a backup device. Values are from 8 through 254. In VRRP, the default backup device priority is 100, and the owner device has a default priority of 255. In VRRP-E, the default backup device priority is 100.

track-priority *value*

Sets the new priority value if the interface goes down. Values are from 1 through 254. Default is 2 for VRRP, and default is 5 for VRRP-E.

Modes

VRID interface configuration mode

Usage Guidelines

In VRRP, the backup device with the highest priority assumes the role of VRRP master device if the owner device fails. The interface on which the Virtual Routing ID (VRID) is configured must be in the same subnet (but not be the same address) as the IP address associated with the VRID by the owner device.

In VRRP-E, all devices are configured as backup devices and the backup device with the highest priority becomes the master device. If the master device fails, the backup device with the highest priority at that time assumes the role of VRRP master device. The IP address assigned to the interface of any device in the same virtual router must be in the same IP subnet. The IP address assigned to the VRID must not be configured on any of the Brocade devices.

This command must be entered before the **ip-address** command can be configured for a VRRP or VRRP-E virtual routing ID.

The **no** form of this command removes the virtual router configuration.

Examples

The following example configures the device as a VRRP backup device and assigns it a priority of 110.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.3/24
device(config-if-e1000-1/5)# ip vrrp vrid 1
device(config-if-e1000-1/5-vrid-1)# backup priority 110
device(config-if-e1000-1/5-vrid-1)# advertise backup
device(config-if-e1000-1/5-vrid-1)# ip-address 10.53.5.254
device(config-if-e1000-1/5-vrid-1)# activate
```

The following example configures the device as a VRRP-E backup device and assigns it a priority of 50 and a track priority of 10.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.10.4/24
device(config-if-e1000-1/5)# ip vrrp vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 50 track-priority 10
device(config-if-e1000-1/5-vrid-2)# ip-address 10.53.10.254
device(config-if-e1000-1/5-vrid-2)# activate
```

backup (VSRP)

Configures the device as a VSRP backup for the VRID or changes the backup priority and the track priority.

Syntax

backup [**priority** *priority-number* [**track-priority** *track-number*]]

no backup [**priority** *priority-number* [**track-priority** *track-number*]]

Command Default

The default backup priority for the VSRP VRID is 100.

The default track priority for all track ports is 1.

Parameters

priority *priority-number*

Configures the backup priority for the VSRP VRID. The range is from 8 to 255. The default is 100.

track-priority *track-number*

Configures the track priority for the VSRP VRID. The range is from 1 to 255. The default value is 1.

Modes

VSRP VRID configuration mode

Usage Guidelines

This configuration is important because in VSRP, all devices on which a VRID are configured are backups. The master is then elected based on the VSRP priority of each device. There is no "owner" device as there is in VRRP.

The backup priority is used for election of the master. The VSRP backup with the highest priority value for the VRID is elected as the master for that VRID. If two or more backups are tied with the highest priority, the backup with the highest IP address becomes the master for the VRID.

The track priority is used with the track port feature. When you configure a VRID to track the link state of other interfaces, if one of the tracked interface goes down, the software changes the VSRP priority of the VRID interface. The software reduces the VRID priority by the amount of the priority of the tracked interface that went down. For example, if the VSRP interface priority is 100 and a tracked interface with track priority 60 goes down, the software changes the VSRP interface priority to 40. If another tracked interface goes down, the software reduces the VRID priority again, by the amount of the tracked interface track priority.

The **no** form of the command without any options removes the device as the backup. The **no** form of the command with the options resets the backup priority value and the track priority value to the default values.

Examples

The following example configures the backup priority as 75.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# backup priority 75
device(config-vlan-200-vrid-1)# activate
```

The following example configures the backup priority as 100 and the track priority as 2.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# backup priority 100 track-priority 2
device(config-vlan-200-vrid-1)# activate
```

backup-bw-best-effort

Configures bandwidth requirement's interpretation as 'best effort' for backup of all FRR LSPs initiated on this router.

Syntax

backup-bw-best-effort

no backup-bw-best-effort

Command Default

By default, this is not turned on ('Guarantee' mode). The bandwidth requested on the backup for FRR LSPs is a strict requirement that needs to be guaranteed by the router.

Modes

MPLS RSVP configuration mode.

Usage Guidelines

Configuring this command dictates this router to consider the bandwidth requested by FRR LSPs on their backup as a 'best-effort' requirement. So, if a backup with the requested bandwidth could not be setup as per the process described in previous sections, then a backup without any bandwidth is tried to setup instead.

This configuration is only available on a global level, and affects all the FRR LSPs passing through this router for which this router is acting as a PLR.

The **no** form of the command brings the router functionality back to default ("Guarantee" mode) and removes the configuration statement. Consider the bandwidth requested on the backup for FRR LSPs as a strict requirement.

Examples

The following example shows the **backup-bw-best-effort** command.

```
device(config-mpls-rsvp)# backup-bw-best-effort
```

History

Release version	Command history
5.8.00	This command was introduced.

backup-hello-interval

Configures the interval at which backup Virtual Router Redundancy Protocol (VRRP) routers advertise their existence to the master router.

Syntax

backup-hello-interval *seconds*

no backup-hello-interval *seconds*

Command Default

The default backup hello interval is 60 seconds.

Parameters

seconds

The interval, in seconds, at which a backup VRRP router advertises its existence to the master router. Valid values range from 60 through 3600.

Modes

VRID interface 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 router within a designated amount of time, the backup router with the highest priority can assume the role of master.

The **backup-hello-interval** command is configured only on VRRP backup routers and is supported by VRRP and VRRP Extended (VRRP-E).

The **no** form disables the advertisement of a VRRP backup router to a VRRP master router.

Examples

The following example enables advertisements from the VRRP backup router and sets the hello message interval to 80 seconds.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# backup priority 90
device(config-if-e1000-1/6-vrid-1)# advertise backup
device(config-if-e1000-1/6-vrid-1)# backup-hello-interval 80
```

backup-hello-interval (vsrp)

Configures the time interval during which Hello messages are sent by the backup.

Syntax

backup-hello-interval *number*

no backup-hello-interval *number*

Command Default

The backup sends a Hello message to the master every 600 units of 100 milliseconds by default.

Parameters

number

Specifies the time interval for the backup to send the Hello messages. The time range is from 600 through 3600 units of 100 milliseconds.

Modes

VSRP VRID configuration mode

Usage Guidelines

The **no** form of the command resets the time interval to the default value.

Examples

The following example changes the Hello message time interval.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vsrp-1)# backup-hello-interval 600
```

bandwidth

Configures the LSP to inherit bandwidth from its protected LSP configuration.

Syntax

bandwidth { **inherit** | *dec* }

no bandwidth { **inherit** | *dec* }

Command Default

By default, this is not configured. The backup of the FRR LSP does not inherit bandwidth information from protected LSP.

Parameters

inherit *dec*

Inherits bandwidth for detour/backup LSP from the protected LSP.

Modes

MPLS configuration mode (config-mpls-lsp-frr).

Usage Guidelines

The **no** form of the command stops inheriting the bandwidth information from the protected LSP path and removes the configuration statement.

Configuring this command dictates the backup LSP path to inherit the same amount of bandwidth as that of the signaled protected LSP.

For adaptive LSPs, this configuration can be changed on the fly without disabling the LSP first. Committing the configuration changes triggers a make-before-break.

Examples

Display output of the **bandwidth** command:

```
device# show mpls config lsp to_NY
 lsp to_NY
  to 28.28.28.28
  primary to-10-3_hop
  traffic-eng mean-rate 2000
  frr
    bandwidth inherit
  enable
```

Release version	Command history
5.8.00	This command is introduced.

bandwidth-ceiling

Adds a new threshold change point to the autobw-threshold table.

Syntax

bandwidth-ceiling [*bw_in_kbps* | *max*] **threshold** *threshold_in_kbps*

no bandwidth-ceiling [*bw_in_kbps* | | *max*] **threshold** *threshold_in_kbps*

Parameters

bw_in_kbps

Defines the bandwidth ceiling in kilobytes per second. The range is 0 - 2, 147, 483, 647 kilobytes per second.

max

Defines the threshold for any traffic-rate as infinity.

threshold *threshold_in_kbps*

Sets the threshold to be used up to this defined ceiling.

Modes

MPLS auto-bandwidth threshold table configuration mode.

Usage Guidelines

This command adds a new threshold change point to the autobw-threshold table. If the change point is already there, the value of the threshold is updated.

The **no** form of the command removes the bandwidth ceiling entry from the table.

Examples

The following example shows how to set the adjustment=threshold table.

```
device(config)# router mpls
device(config-mpls)# autobw-threshold-table
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 10 threshold 2000
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 1000 threshold 3000
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 10000 threshold 5000
```

The following example shows how to remove one of the threshold entries.

```
device(config)# router mpls
device(config-mpls)# autobw-threshold-table
device(config-mpls-autobw-threshold-table)# no bandwidth-ceiling 1000 threshold 3000
```

The following example shows how to clear the threshold table.

```
device(config)# router mpls
device(config-mpls)# no autobw-threshold-table
```

History

Release	Command history
5.6.00	This command was introduced.

bandwidth-ceiling max threshold percentage

Sets the threshold for any traffic-rate above the maximum bandwidth-ceiling configured in the table as a percentage.

Syntax

bandwidth-ceiling max threshold [*dec* | **percentage***dec*]

no bandwidth-ceiling max threshold [*dec* | **percentage***dec*]

Parameters

max Any rate above the maximum ceiling configured. By default, the last ceiling is used.

dec

Sets the threshold value. Range 0 - 2, 147, 483, 647 kilobits per second.

threshold

Sets the threshold to be used up to this ceiling.

percentage*dec*

Sets the specified threshold value in percentage. Range is 0 - 100%.

Modes

MPLS auto-bandwidth threshold table configuration mode.

Usage Guidelines

The **no** function of this command removes the entry.

Examples

The following example shows how to set the maximum bandwidth percentage to 10.

```
device(config)# router mpls
device(config-mpls)# autobw-threshold-table
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling max threshold percentage 10
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling max threshold 10000
```

History

Release	Command history
05.6.00	The command was introduced.

base vrf

Configures the VRF to which the tunnel source and destination belongs.

Syntax

base vrf *base-vrf-name*

no base vrf *base-vrf-name*

Command Default

By default, the base VRF is not configured. The default VRF is considered the base VRF.

Parameters

base-vrf-name

Specifies the VRF name of the base network.

Modes

Tunnel interface configuration mode

Usage Guidelines

The **no** form of the command disables the base VRF configuration for the tunnel interface.

When the tunnel source interface is configured, the base VRF is checked and if the source interface does not belong to the configured base VRF, a configuration error message is displayed.

Examples

The following example configures the base VRF for the tunnel interface.

```
device(config)# interface ethernet 3/1
device(config-int-e10000-3/1)# ip address 36.0.8.108/32
device(config-int-e10000-3/1)# exit
device(config)# interface tunnel 1
device(config-tnif-1)# base vrf vrf1
```

History

Release version	Command history
05.8.00	This command was introduced.

bfd

Configures Bidirectional Forwarding Detection (BFD) session parameters on BGP-enabled interfaces.

Syntax

bfd min-tx *transmit-time* **min-rx** *receive-time* **multiplier** *number*

no bfd min-tx *transmit-time* **min-rx** *receive-time* **multiplier** *number*

Command Default

Default parameters are used.

Parameters

min-tx *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 1000 unless changed using the **bfd interval** command in interface sub-type configuration mode.

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 1000 unless changed using the **bfd interval** command in interface sub-type configuration mode.

multiplier *number*

Specifies the number of consecutive BFD control packets that must be missed by the BFD peer before the BFD peer determines that the connection is not operational. Valid values range from 3 through 50. The default is 3.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

When using BFD for BGP, you must configure BFD globally at the router BGP level. You can also use this configuration to set new default values for the transmit interval, receive interval, and for the detection time multiplier.

For a single-hop EBGP session, the BFD parameters configured under interface subtype configuration mode are used because the BFD session for a single hop is also shared with other applications. To create a BFD session for a single-hop BGP session, you must first enable BFD and configure the timers for the interface on which single-hop BGP peering is established using the **bfd interval**command in interface subtype configuration mode.

For multihop BFD sessions, BFD does not need to be enabled for any of the interfaces, and the BFD timers need not be configured, because the default values can be used.

The **min-tx**, **min-rx**, and **multiplier** keywords can also be configured for each peer and peer group and will override the global configuration.

When Brocade NetIron CER Series or Brocade NetIron CES Series devices are heavily loaded or under stress, BFD sessions may flap if the configured BFD interval is less than 500 milliseconds with a multiplier value of 3.

The *transmit-time* and *receive-time* variables are the intervals desired by the local device. The actual values in use will be the negotiated values.

The **no** form of the command globally removes BFD for BGP parameters from the device.

Examples

The following example sets the BFD session parameters globally for BGP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# bfd min-tx 120 min-rx 150 multiplier 8
```

The following example sets the BFD session parameters globally for BGP for VRF "red" in BGP address-family IPv4 unicast VRF configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# bfd min-tx 120 min-rx 150 multiplier 8
```

bfd all-interfaces

Enables Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process.

Syntax

bfd all-interfaces all-vrfs

bfd all-interfaces

no bfd all-interfaces all-vrfs

no bfd all-interfaces

Command Default

BFD is disabled by default.

Parameters

all-vrfs

Specifies all VRFs.

Modes

IS-IS router configuration mode

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Although this command configures BFD for OSPFv2 on all OSPFv2-enabled interfaces for a device, it is not required if you use the **ip ospf bfd** command to configure specific interfaces. It can be used independently or together with the **ip ospf bfd** command.

Although this command configures BFD for OSPFv3 on all OSPFv3-enabled interfaces for a device, it is not required if you use the **ipv6 ospf bfd** command to configure specific interfaces. It can be used independently or together with the **ipv6 ospf bfd** command.

Although this command configures BFD for IS-IS on all IS-IS-enabled interfaces for a device, it is not required if you use the **isis bfd** command to configure specific interfaces. It can be used independently or together with the **isis bfd** command.

The **all-vrfs** keyword is only available in OSPF router configuration mode and OSPF router VRF configuration mode.

The **no** form of the command in OSPF router configuration mode disables BFD on all OSPFv2-enabled interfaces. The **no** form of the command in OSPFv3 router configuration mode disables BFD on all OSPFv3-enabled interfaces. The **no** form of the command in IS-IS router configuration mode disables BFD on all IS-IS-enabled interfaces.

Examples

The following example enables BFD globally for all VRFs on all OSPFv2-enabled interfaces.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# bfd all-interfaces all-vrfs
```

The following example enables BFD globally on all OSPFv2-enabled interfaces for VRF instance “red”.

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

The following example disables BFD globally on all OSPFv3-enabled interfaces.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# no bfd all-interfaces
```

The following example enables BFD on all IS-IS-enabled interfaces.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# bfd all-interfaces
```

bfd holdover-interval

Sets the time interval for which BFD session down notifications are delayed before a routing protocol is notified that a BFD session is down.

Syntax

bfd holdover-interval *time*

no bfd holdover-interval *time*

Command Default

The BFD holdover interval is set to 0 by default.

Parameters

time

Specifies the BFD holdover interval in seconds. In the BGP and BGP address-family IPv4 unicast VRF configuration modes, valid values range from 1 through 30, and the default is 0. In the IS-IS router, OSPF router, OSPFv3 router, and OSPF router VRF configuration modes, valid values range from 1 through 20, and the default is 0.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

IS-IS router configuration mode

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

For BGP, the BFD holdover interval is supported for both single-hop and multihop sessions. For OSPF and IS-IS, the BFD holdover interval is supported for single-hop sessions only.

In BGP configuration mode, use this command to set the BFD holdover-time interval globally for BGP. In IS-IS router configuration mode, use this command to set the BFD holdover-time interval globally for IS-IS. In OSPF router configuration mode, use this command to set the BFD holdover-time interval globally for OSPFv2. In OSPFv3 router configuration mode, use this command to set the BFD holdover-time interval globally for OSPFv3.

The holdover interval on BGP-enabled interfaces can be configured globally, on each peer, or peer-group.

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)# bfd holdover-interval 15
```

The following example sets the BFD holdover interval globally to 15 for VRF instance “red” in BGP address-family IPv4 unicast VRF configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# 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-ospf-router)# bfd holdover-interval 12
```

The following example sets the BFD holdover interval globally 12 for VRF instance “red” in OSPF router VRF configuration mode.

```
device# configure terminal
device(config)# router ospf vrf red
device(config-ospf-router-vrf-red)# 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-ospf6-router)# bfd holdover-interval 20
```

The following example sets the BFD holdover interval globally to 20 in IS-IS router configuration mode.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# bfd holdover-interval 20
```

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*

Command Default

Default parameters are used.

Parameters

interval *transmit-time*

Specifies the interval, in milliseconds, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000.

min-rx *receive-time*

Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000.

multiplier *number*

Specifies the number of consecutive BFD control packets that must be missed by a BFD peer before the peer determines that the connection is not operational. Valid values range from 3 through 50.

Modes

Interface subtype 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.

When Brocade NetIron CER Series or Brocade NetIron CES Series devices are heavily loaded or under stress, BFD sessions may flap if the configured BFD interval is less than 500 milliseconds with a multiplier value of 3.

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 1/1
device(config-if-e1000-1/1)# bfd interval 100 min-rx 100 multiplier 4
```

bfd-enable

Enables Bidirectional Forwarding Detection (BFD) globally on BGP-enabled interfaces.

Syntax

bfd-enable

no bfd-enable

Command Default

BFD is disabled by default.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

If BFD for BGP is globally disabled and then enabled, the original BFD sessions for BGP may not be available, depending on whether the maximum BFD sessions limit has been reached. When a BFD session for BGP is disabled, the session is removed but BGP peering does not go down. The remote BFD peer is informed that BFD use is disabled.

This command overrides all other BGP BFD configurations.

The **no** form of this command disables BFD globally and terminates all BFD sessions used by BGP.

Examples

The following example enables BFD globally for BGP.

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

The following example enables BFD globally for BGP4 for VRF "red" in BGP address-family IPv4 unicast VRF configuration mode.

```
device# configure terminal
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# bfd-enable
```

bfd mh-session-setup-delay

Provides a time delay before establishing the multihop BFD session after the system initializes.

Syntax

bfd mh-session-setup-delay *seconds*

no bfd mh-session-setup-delay *seconds*

Command Default

By default, the time delay to establish the multihop session is set to 0 seconds.

Parameters

seconds

The time delay in seconds. You can specify a value between 0 and 600 seconds. The default value is 0 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the time delay for the multihop session.

Examples

The following example sets a delay time of 90 seconds before establishing the multihop session.

```
device(config)#bfd mh-session-setup-delay 90
```

History

Release version	Command history
05.7.00	This command was introduced.

bfd sh-session-setup-delay

Provides a time delay before establishing the single hop BFD session after the port is enabled.

Syntax

bfd sh-session-setup-delay *seconds*

no bfd sh-session-setup-delay *seconds*

Command Default

By default, the time delay to establish the single hop session is set to 180 seconds.

Parameters

seconds

The time delay in seconds. You can specify a value between 0 and 600 seconds. The default value is 180 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the time delay for the session.

Examples

The following example sets a delay time of 40 seconds before establishing the single hop session.

```
device(config)# bfd sh-session-setup-delay 40
```

History

Release version	Command history
5.7.00	This command was introduced.

cam ifsr

Disables or enables In-Field Soft Repair (IFSR) for TCAM hardware errors for a specified host name.

Syntax

cam ifsr { **disable** | **enable** }

Command Default

Parameters

disable

Disables IFSR for TCAM hardware errors for a specified host name.

enable

Enables IFSR for TCAM hardware errors for a specified host name.

Modes

Global configuration mode

Usage Guidelines

Use this to command to disable or enable persistent hardware errors from displaying on the console as syslog messages as a result of hardware errors. Some hardware errors cannot be repaired. Continuous syslog messages will appear on the console displaying the system KBP errors. The command allows you to disable the feature, and stop the monitoring of hardware errors. After replacing the hardware, enable the feature. By default, the command is enabled.

The IFSR feature is supported only on the following interface modules for Brocade MLX Series devices.

- BR-MLX-100Gx2-CFP2-X2
- BR-MLX-10Gx20-M (1G/10G combo) and BR-MLX-10Gx20-X2 (1G/10G combo)
- BR-MLX-10Gx4-IPSEC-M

Examples

The following example enables IFSR.

```
device(config)# cam ifsr enable
```

The following example disables IFSR on slot 3 of the LP module.

```
device(config)# cam ifsr disable
IFSR is disabled on slot 3
```

History

Release version	Command history
05.8.00a	This command was introduced.

cam-mode amod

Enables Algorithmic mode which optimizes the CAM space and power utilization and achieves -X2 CAM profile numbers.

Syntax

cam-mode amod slot *number*

no cam-mode amod slot *number*

Command Default

The TCAM mode (non-Algorithmic mode) is enabled by default.

Parameters

slot

Specifies the line processor (LP) slot on which Algorithmic mode must be enabled.

number

Specifies the slot number.

Modes

Global configuration mode

Usage Guidelines

The line card must be reloaded for Algorithmic mode to take effect.

By default, BR-MLX-100Gx2-CFP2-X2, BR-MLX-10Gx20-X2, and BR-MLX-1GX20-U10G-X2 cards boot up with -M CAM profile numbers and if uRPF is enabled, the number of routes are reduced by half. You must enable Algorithmic mode to achieve -X2 CAM profile numbers. Algorithmic mode also supports uRPF mode to work without reducing the route scale.

The configuration will be ignored at the LP if the command is applied on a slot other than BR-MLX-100Gx2-CFP2-X2, BR-MLX-10Gx20-X2, and BR-MLX-1GX20-U10G-X2.

If Algorithmic mode is enabled on an empty slot, the line card inserted at a later stage will be initialized to Algorithmic mode.

The **no** form of the command disables Algorithmic mode.

NOTE
Algorithmic mode is supported on MR2-X management modules only.

Examples

The following example configures Algorithmic mode on slot 2.

```
device# configure terminal
device(config)# cam-mode amod slot 2
```

History

Release version	Command history
05.8.00a	This command was introduced.

capability as4

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

Syntax

capability as4-enable { **disable** | **enable** }

no capability

Command Default

This feature is disabled.

Parameters

disable

Disables 4-byte autonomous system number (ASN) capability.

enable

Enables 4-byte autonomous system number (ASN) capability.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to disable this functionality.

Examples

The following example enables 4-byte ASN capability.

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

clear access-list receive accounting

Clears IPv4 receive access-control list (rACL) accounting statistics.

Syntax

clear access-list receive accounting { **all** | **name** *acl-name* }

Parameters

all

Specifies clearing accounting statistics for all configured IPv4 rACLs.

name *acl-name*

Clears accounting statistics for the specified IPv4 rACL.

Modes

Privileged EXEC mode.

Usage Guidelines

This command is also available in global configuration mode.

Examples

The following example clears accounting statistics for an IPv4 rACL named acl_ext1.

```
device(config)# clear access-list receive accounting name act-ext1
```

History

Release	Command History
5.6.00	This command was introduced.

clear arp-guard-statistics

Clears the different statistical information of the ARP guard.

Syntax

clear arp-guard statistics ethernet { **all** | [**ethernet** *slot/port* [**vlan** *vlan-id*] } | **all**]

Command Default

Clears all statistics related to the ARP guard.

Parameters

all

Clears all ARP guard statistics.

ethernet *slot/port*

Specifies the defined Ethernet port to clear.

vlan*vlan_id*

Specifies the defined VLAN information to clear. The VLAN ID range is between 1 and 4090.

Modes

EXEC mode.

Usage Guidelines

Use the **show arp-guard statistics** command to verify changes after executing the **clear arp-guard statistics** command.

Examples

The following example indicates clearing statistics information for all the ports.

```
Brocade# clear arp-guard-statistics all
Brocade# show arp-guard statistics ethernet all

Port         Vlan-id  Total_Arp_pkts_captured  Total_Arp_pkts_forwarded  Total_Arp_pkts_dropped  LAG :
Prim
1/1  (Def/Untag)1             0                         0                         0
1/1              3             0                         0                         0
1/1              2             0                         0                         0
2/1  (Def/Untag)1             0                         0                         0
2/1              2             0                         0                         0
2/1              4             0                         0                         0
2/1              5             0                         0                         0
```

The following example indicates clearing statistics information for any individual ports.

```
Brocade# clear arp-guard-statistics ethernet 1/1
Brocade# show arp-guard statistics ethernet 1/1

Port         Vlan-id  Total_Arp_pkts_captured  Total_Arp_pkts_forwarded  Total_Arp_pkts_dropped  LAG :
Prim
1/1 (Def/Untag)1             0                         0                                                0
1/1            3             0                         0                                                0
1/1            2             0                         0                                                0
```

The following example indicates clearing statistics information for VLAN ID 2 from port 1/1.

```
Brocade# clear arp-guard-statistics ethernet 1/1 vlan 2
Brocade# show arp-guard statistics ethernet 1/1 vlan 2

Port         Vlan-id  Total_Arp_pkts_captured  Total_Arp_pkts_forwarded  Total_Arp_pkts_dropped  LAG :
Prim
1/1            2               0                         0                      0
```

History

Release version	Command history
5.7.00	This command was introduced.

clear bm histogram

Clears buffer histogram data.

Syntax

clear bm histogram

Modes

Privileged EXEC mode

Usage Guidelines

The histogram information is collected and maintained internally, in a cyclical buffer. It can be reviewed to determine if resource allocation failures or task CPU usage may have contributed to an application failure.

The main objective of the buffer histogram is to see if there was any buffer exhaustion in the last few seconds (10-60sec). Buffer usage is collected when available buffers in the 2K buffer size pool fall below the reserved limit. Before starting another collection cycle, it may be useful to clear the histogram buffers using the **clear bm histogram** command. This command can also be entered in global configuration mode.

Examples

The following example clears buffer histogram data.

```
device# clear bm histogram
```

History

Release	Command History
5.5.00	This command was introduced.

clear cpu histogram sequence

Clears CPU histogram sequential execution of task data.

Syntax

clear cpu histogram sequence

no clear cpu histogram sequence

Modes

Privileged EXEC mode.

Global configuration mode.

Usage Guidelines

The CPU histogram provides information about task CPU usage. The histogram information is collected and maintained internally, in a cyclical buffer. It can be reviewed to determine if resource allocation failures or task CPU usage may have contributed to an application failure.

Before starting another collection cycle of task CPU usage, it may be useful to clear the existing CPU histogram information using the **clear cpu histogram sequence** command. This command can also be entered in global configuration mode.

To view the CPU histogram information, use the **show cpu histogram** command.

Examples

The following example clears the CPU histogram sequential execution of task information.

```
device(config)# clear cpu histogram sequence
```

History

Release	Command History
5.5.00	This command was introduced.

clear dot1x-mka statistics

Clears the 802.1x (dot1x) MACsec Key Agreement (MKA) traffic statistics for the specified interface.

Syntax

clear dot1x-mka statistics ethernet *slot*/*port*

Parameters

ethernet *slot port*

Specifies an Ethernet interface and its slot on the device, and interface on the slot.

Modes

Privileged EXEC mode

Examples

In the following example, dot1x-MKA traffic statistics are cleared for interface 3/2.

```
device(config)# clear dot1x-mka statistics ethernet 3/2
dot1x-MKA statistics cleared
```

History

Release version	Command history
5.8.00	This command was introduced.

clear ikev2 statistics

Clears Internet Key Exchange version 2 (IKEv2) statistics by resetting the various IKEv2 counters to zero.

Syntax

clear ikev2 statistics

Modes

Privileged EXEC mode

Examples

The following example clears IKEv2 statistics from the device.

```
device# clear ikev2 statistics
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00	This command was modified to add support for IPsec IPv6.

clear ikev2 sa

Clears Internet Key Exchange version 2 security associations (IKEv2 SAs).

Syntax

clear ikev2 sa [**fvrf** *vrf-name* | **ipv4** | **ipv6** | **local** *ip-address* | **remote** *ip-address*]

Parameters

fvrf *vrf-name*
Specifies the front-door VRF (FVRF) for the SAs.

ipv4
Specifies clearing IPv4 connections.

ipv6
Specifies clearing IPv6 connections.

local *ip-address*
Specifies the IP address for the local interface. Both IPv4 and IPv6 address formats are supported.

remote *ip-address*
Specifies the IP address for the remote interface. Both IPv4 and IPv6 address formats are supported.

Modes

Privileged EXEC mode

Usage Guidelines

The clearing process deletes and re-establishes the SAs (including any child SAs).

When optional parameters are not specified, the command clears all IKEv2 SAs on the device.

Examples

The following example clears the IKEv2 SAs for local interface 10.10.20.1.

```
device# clear ikev2 sa local 10.10.20.1
```

The following example clears the IKE SAs for remote interface 10.0.10.1.

```
device# clear ikev2 sa remote 10.0.10.1
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00	This command was modified to add support for IKEv2 IPv6.

clear ip bgp dampening

Reactivates suppressed BGP4 routes.

Syntax

clear ip bgp dampening [*ip-addr* { **/** *mask* }]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

IPv4 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

The following example unsuppresses all suppressed BGP4 routes.

```
device# clear ip bgp dampening
```

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*]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv4 mask of a specified route in CIDR notation.

neighbor

Clears dampening statistics only for routes learned from the specified neighbor.

ip-addr

IPv4 address of the neighbor.

regular-expression

Specifies a regular expression.

string

Regular expression.

Modes

Privileged EXEC mode

Examples

This example clears the dampening statistics for a BGP4 route.

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

clear ip bgp local routes

Clears BGP4 local routes from the IP route table and resets the routes.

Syntax

clear ip bgp local routes

Modes

Privileged EXEC mode

Examples

This example clears all BGP4 local routes.

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

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* | *peer-group-name* | *ip-addr* } [**last-packet-with-error**] [**notification-errors**] [**soft** [**in** | **out**]] [**soft-outbound**] [**traffic**]

Parameters

all

Resets and clears all BGP4 connections to all neighbors.

as-num

Clears all BGP4 connections within this autonomous system. Range is from 1 through 4294967295.

peer-group-name

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

ip-addr

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

last-packet-with-error

Clears all BGP4 connections identified as having the last packet received with an error.

notification-errors

Clears all BGP4 connections identified as having notification errors.

soft

Refreshes routes received from or sent to the neighbor.

in

Refreshes received routes.

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.

Modes

Privileged EXEC mode

Examples

The following example refreshes all BGP4 neighbor connections.

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

clear ip bgp routes

Clears BGP4 routes from the IP route table and resets the routes.

Syntax

clear ip bgp routes [*ip-addr* [**/** *mask*]]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv4 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4 routes.

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

clear ip bgp traffic

Clears the BGP4 message counter for all neighbors.

Syntax

clear ip bgp traffic

Modes

Privileged EXEC mode

Examples

The following example clears the BGP4 message counters:

```
device# clear ip bgp traffic
```

clear ip bgp vrf

Clears BGP4 information for a virtual routing and forwarding (VRF) instance.

Syntax

clear ip bgp vrf *vrf-name*

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example clears BGP4 information for VRF red.

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

clear ip ospf

Clears OSPF process, counters, neighbors, or routes.

Syntax

clear ip ospf all

clear ip ospf neighbor { *A.B.C.D* | **all** } [**ethernet** *slot/port* | **tunnel** *number* | **ve** *vlan_id*]

clear ip ospf routes { *A.B.C.D/L* | **all** }

clear ip ospf shortcut registration

clear ip ospf traffic

Parameters

all

Globally resets (disables then re-enables) OSPF without deleting the OSPF configuration information.

neighbor

Clears the specified neighbor, or clears all neighbors.

A.B.C.D

Specifies the IP address of the neighbor to clear.

all

Clears all neighbors.

ethernet *slot/port*

Specifies the Ethernet interface and the interface ID in the format slot/port.

tunnel *number*

Specifies a tunnel.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

routes

Clears matching routes or clears all routes.

A.B.C.D

Clears all routes that match the prefix and mask that you specify.

all

Clears all routes.

shortcut registration

Clears OSPF shortcuts and re-registers OSPF with MPLS.

traffic

Clears OSPF counters and errors.

Modes

User EXEC mode

Examples

The following example resets OSPF without deleting the OSPF configuration.

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

clear ip vrrp statistics

Clears IPv4 Virtual Router Redundancy Protocol (VRRP) statistics.

Syntax

clear ip vrrp statistics

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring VRRP options, for example, and want to clear existing statistics.

Examples

The following example clears IPv4 VRRP statistics when entered in privileged EXEC mode.

```
device# clear ip vrrp statistics
```

The following example clears IPv4 VRRP statistics when entered in VRID interface configuration mode.

```
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# clear ip vrrp statistics
```

clear ip vrrp-extended statistics

Clears IPv4 Virtual Router Redundancy Protocol (VRRP) Extended (VRRP-E) statistics.

Syntax

clear ip vrrp-extended statistics

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring VRRP-E options, for example, and want to clear existing statistics.

Examples

The following example clears IPv4 VRRP-E statistics when entered in privileged EXEC mode.

```
device# clear ip vrrp-extended statistics
```

The following example clears IPv4 VRRP-E statistics when entered in VRID interface configuration mode.

```
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.4.1/24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# clear ip vrrp-extended statistics
```

clear ipsec error-count

Clears the error counters for the IPsec errors.

Syntax

clear ipsec error-count

Modes

Privileged EXEC mode.

Examples

The following example clears the error counters for the IPsec errors.

```
device# clear ipsec error-count
```

History

Release version	Command history
5.8.00	This command was introduced.

clear ipsec sa

Clears IPsec security associations (SAs).

Syntax

clear ipsec sa [**fvrf** *vrf-name* | **ipv4** | **ipv6** | **peer** *ip-address*]

Parameters

fvrf *vrf-name*
: Specifies the front-door VRF (FVRF) for the SAs.

ipv4
: Specifies clearing IPv4 associations.

ipv6
: Specifies clearing IPv6 associations.

peer *ip-address*
: Specifies the IP address for the peer interface. Both IPv4 and IPv6 address formats are supported.

Modes

Privileged EXEC mode

Usage Guidelines

The clearing process deletes and re-establishes IPsec SAs. The SAs remain unchanged.

When optional parameters are not specified, this command clears all IPsec SAs on the device.

Examples

The following example clears all IPsec SAs on the device.

```
device# clear ipsec sa
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00	This command was modified to add support for IPsec IPv6.

clear ipsec statistics

Clears IPsec system counters (such as ESP packet counts and IPsec error counts), and IPsec tunnel packet and byte counts (such as transmitted and received packets).

Syntax

clear ipsec statistics [**all**]

Parameters

all

(Optional) Specifies that all IPsec statistics should be cleared (this includes system counters and IPsec tunnel packet counts and byte counts).

Modes

Privileged EXEC mode.

Usage Guidelines

This command supports IPsec IPv4 and IPv6.

When you omit the optional **all** parameter, only the system counters (such as ESP packet counts and IPsec error counts) are cleared. When you include the **all** parameter, the system counters and IPsec tunnel packet and byte counts are also cleared.

Examples

The following example clears the IPSec system counters.

```
device# clear ipsec statistics
```

The following example clears all of the IPsec statistics, including system counters and IPsec tunnel packet and byte counts.

```
device# clear ipsec statistics all
```

History

Release version	Command history
5.8.00	This command was modified to add the **all** keyword.
5.9.00	This command was modified to add support for IPsec IPv6.

clear ipsec statistics tunnel

Clears the IPsec tunnel packet and bytes counters.

Syntax

clear ipsec statistics tunnel *dec* | **all**

Parameters

dec

Clears the IPsec counter for the tunnel specified by its ID number.

all

Clears the IPsec counters for all tunnels.

Modes

User EXEC mode.

Privileged EXEC mode.

Examples

The following example clears the IPsec tunnel packet and bytes counters.

```
device# clear ipsec statistics tunnel
```

History

Release version	Command history
5.8.00	This command was introduced.

clear ipv6 bgp dampening

Reactivates suppressed BGP4+ routes.

Syntax

clear ipv6 bgp dampening [*ipv6-addr* { **/** *mask* }]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

IPv6mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

The following example unsuppresses all suppressed BGP4+ routes.

```
device# clear ipv6 bgp dampening
```

clear ipv6 bgp flap-statistics

Clears the dampening statistics for a BGP4+ route without changing the dampening status of the route.

Syntax

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

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv6 mask of a specified route in CIDR notation.

neighbor

Clears dampening 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.

Modes

Privileged EXEC mode

Examples

This example clears the dampening statistics for a BGP4+ route.

```
device# clear ip bgp flap-statistics 2001:2002::23:61
```

clear ipv6 bgp local routes

Clears BGP4+ local routes from the IP route table and resets the routes.

Syntax

clear ipv6 bgp local routes

Modes

Privileged EXEC mode

Examples

This example clears all BGP4+ local routes.

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

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* | *iipv6-addr* } [**last-packet-with-error**] [**notification-errors**] [**soft** [**in** | **out**]] [**soft-outbound**] [**traffic**]

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.

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.

Modes

Privileged EXEC mode

Examples

The following example refreshes all BGP4+ neighbor connections.

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

clear ipv6 bgp routes

Clears BGP4+ routes from the route table and resets the routes.

Syntax

clear ipv6 bgp routes [*ipv6-addr* { **/** *mask* }]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv6 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4+ routes.

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

clear ipv6 bgp traffic

Clears the BGP4+ message counter for all neighbors.

Syntax

clear ipv6 bgp traffic

Modes

Privileged EXEC mode

Examples

The following example clears the BGP4+ message counters.

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

clear ipv6 ospf

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

Syntax

clear ipv6 ospf all

clear ipv6 ospf counts

clear ipv6 ospf counts neighbor *A.B.C.D*

clear ipv6 ospf counts neighbor interface { **ethernet** *slot/port* | **ve** *vlan_id* } [*A.B.C.D*]

clear ipv6 ospf { **force-spf** | **redistribution** | **traffic** } [**vrf** *vrf-name*]

clear ipv6 ospf neighbor all

clear ipv6 ospf neighbor interface { **ethernet** *slot/port* | **ve** *vlan_id* } [*A.B.C.D*]

clear ipv6 ospf routes { *IPv6addr* | **all** }

Command Default

Disabled.

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.

interface

Specifies an interface.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

force-spf

Performs the shortest path first (SPF) calculation without clearing the OSPFv3 database.

redistribution

Clears OSPFv3 redistributed routes.

traffic

Clears OSPFv3 traffic statistics.

routes

Clears OSPFv3 routes.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **force-spf** keyword to perform the shortest path first (SPF) calculation without clearing the OSPFv3 database.

Examples

The following example restarts the OSPFv3 processes.

```
device# clear ipv6 ospf all
```

The following example clears all OSPFv3 counters for a specified neighbor.

```
device# clear ipv6 ospf counts neighbor 10.10.10.1
```

clear ipv6 vrrp statistics

Clears IPv6 Virtual Router Redundancy Protocol (VRRP) statistics.

Syntax

clear ipv6 vrrp statistics

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring IPv6 VRRP options, for example, and want to clear existing VRRP statistics.

Examples

The following example clears IPv6 VRRP statistics when entered in privileged EXEC mode.

```
device# clear ipv6 vrrp statistics
```

The following example clears IPv6 VRRP statistics when entered in VRID interface configuration mode.

```
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ipv6 vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# clear ipv6 vrrp statistics
```

clear ipv6 vrrp-extended statistics

Clears IPv6 Virtual Router Redundancy Protocol (VRRP) Extended (VRRP-E) statistics.

Syntax

clear ipv6 vrrp-extended statistics

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring IPv6 VRRP-E options, for example, and want to clear existing VRRP-E statistics.

Examples

The following example clears IPv6 VRRP-E statistics when entered in privileged EXEC mode.

```
device# clear ipv6 vrrp-extended statistics
```

The following example clears IPv6 VRRP-E statistics when entered in VRID interface configuration mode.

```
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 2001:DB8::2/24
device(config-if-e1000-1/5)# ipv6 vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# clear ipv6 vrrp-extended statistics
```

clear isis shortcut

Clears IS-IS shortcuts on LSPs. IS-IS attempts to re-map the LSP To address to the IS-IS system ID.

Syntax

clear isis shortcut [**lsp** *lsp-name* | **registration**]

Parameters

lsp *lsp-name*
Clears the IS-IS shortcuts from the specified LSP.

registration
Reregisters IS-IS with MPLS.

Modes

Privileged EXEC mode.

Usage Guidelines

NOTE
The clearing of IS-IS shortcuts is not a common operation.

Clearing shortcuts is useful when the mapping between the To address and System ID must be refreshed after the LSP tunnel is being used in the SPF calculation.

If you do not specify an LSP, the command clears all IS-IS shortcuts from the configuration.

Examples

The following example shows the clearing of IS-IS shortcuts for the tunnel3 LSP.

```
device# clear isis shortcut lsp tunnel3
```

clear mac-address vpls

Clears the VPLS MAC entries on the Brocade device.

Syntax

clear mac-address vpls

clear mac-address vpls ethernet *slot/port vlan-id* [**inner-vlan** *number* | **isid** *number*]

clear mac-address vpls id *vpls-id* [**mdb remote**]

clear mac-address vpls label *local-number*

clear mac-address vpls mdb [**mdup -stats** | **remote**]

clear mac-address vpls name *vpls-name*]

Parameters

ethernet *slot/port vlan-id*

Clears all VPLS MAC entries on the VLAN port for the specified interface slot and port number, and VLAN ID.

inner-vlan *number*

Clears the VPLS MAC entries for the specified inner VLAN number on the VLAN port.

isid *number*

Clears the VPLS MAC entries for the specified service ID (ISID) number on the VLAN port.

id *vpls-id*

Clears all VPLS MAC entries for the specified VPLS ID.

mdb remote

Clears the cluster remote MDUP entries for the specified VPLS ID.

label *local-number*

Clears all VPLS MAC entries associated with the specified local label.

mdb [**mdup -stats** | **remote**]

Clears all VPLS MAC cluster MDUP statistics and entries.

mdup-stats

Clears the VPLS MAC MDUP statistics.

remote

Clears the VPLS MAC entries for all cluster remote MDUP entries.

name *vpls-name*

Clears all VPLS MAC entries for the specified VPLS instance.

Modes

Privileged EXEC mode

Usage Guidelines

This command allows you to clear the entries in the VPLS MAC database. The **show mac vpls** command displays the database.

Examples

The following example clears the entries stored in the VPLS MAC database belonging to a v1 VPLS instance.

```
device# clear mac-address vpls name v1
```

clear macsec statistics

Clears the MACsec traffic statistics for the specified interface.

Syntax

clear macsec statistics ethernet ethernet *slot*/*port*

Parameters

ethernet *slot/port*

Specifies an Ethernet interface by slot on the device, and interface on the slot.

Modes

Privileged EXEC mode.

Usage Guidelines

This command operates in all modes.

Examples

In the following example, MACsec traffic statistics are cleared for interface 3/2.

```
device(config)# clear macsec statistics ethernet 3/2
MACsec statistics cleared
```

History

Release version	Command history
5.8.00	This command was introduced.

clear memory histogram

Clears memory histogram data.

Syntax

clear memory histogram

Modes

Privileged EXEC mode.

Usage Guidelines

This command operates in all modes.

The memory histogram keeps track of each memory allocation/deallocation request from an application. It helps to identify memory leak and memory usage across the task. It also monitors the under usage condition and reports to the system. The memory histogram is recorded when available memory goes below the threshold limit on each memory pool.

Before starting another collection cycle, it may be useful to clear the existing memory histogram information using the **clear memory histogram sequence** command. This command can also be entered in global configuration mode.

To view the memory histogram information, use the **show memory histogram** command.

Examples

The following example clears memory histogram data.

```
device(config)# clear memory histogram
```

History

Release	Command History
5.5.00	This command was introduced

clear metro mp-vlp-queue

Resets the management processor virtual line card (MP-VLP) queue statistics on Brocade NetIron CER Series devices.

Syntax

clear metro mp-vlp-queue

Modes

Privileged EXEC mode.

Usage Guidelines

this command operates in all modes.

show metro mp-vlp-queue

Examples

This example clears all the counters in the MP-VLP queue statistics.

```
device# clear metro mp-vlp-queue
```

History

Release version	Command history
5.8.00a	This command was introduced.

clear mmrp statistics

Clears MMRP statistics.

Syntax

clear mmrp statistics vlan-id *vlan-num*

Parameters

vlan-id *vlan-num*

Specifies the VLAN ID.

Modes

Privileged EXEC mode

Examples

The following example clears the MMRP statistics.

```
device# clear mmrp statistics
```

clear mpls auto-bandwidth-samples

Deletes the sample-history from the auto-bandwidth LSPs.

Syntax

clear mpls auto-bandwidth-samples [**all** | **lsp** *lsp_name*]

Parameters

all

Clear all of the auto-bandwidth sample history.

lsp *lsp_name*

Clears the auto-bandwidth sample history for the specified LSP.

Modes

Privileged EXEC mode.

Usage Guidelines

Samples are not deleted or deallocated when the LSP is disabled or when auto-bandwidth is disabled at the global or LSP level.

Examples

The following example shows the command used to clear all of the auto-bandwidth sample history.

```
device# clear mpls auto-bandwidth-samples all
```

History

Release	Command history
5.6.00	This command was introduced.

clear mpls ldp neighbor

Resets all LDP sessions on the Brocade device or the LDP sessions for the specified IP address. The LDP sessions are automatically reestablished when at least one Hello adjacency exists with the neighbor, and the LDP configuration remains unchanged.

Syntax

clear mpls ldp neighbor { **all** | *peer-ip-addr* [**label-space-id** *label-space*] }

Parameters

all

All LDP sessions on the Brocade device are reset, including the targeted LDP sessions.

peer-ip-addr

An LDP session. All LDP sessions with the matching peer address is reset.

label-space-id *label-space*

Specifies the label space for the LDP session.

Modes

Privileged EXEC mode

Usage Guidelines

This command allows you to reset the following LDP sessions:

- Platform-wide label space
- Interface specific label space

When an LDP session is terminated as a result of the **clear mpls ldp neighbor** command, the Brocade device does not generate any notification message for the neighbor. Instead, the device unilaterally terminates the session and closes the associated TCP session. The other end of the LDP session detects this reset operation in either of the following two ways:

- TCP session is broken (half connected). The device detects this while receiving or sending LDP messages on TCP socket fails (with fatal error), indicating that underlying TCP session is aborted by remote peer.
- A new TCP connection request is received from the neighbor while the older session is still operational (when this is in the passive role).

NOTE

Either of the previous events trigger the remote end of the LDP session to tear down the session and try to reestablish it. Resetting an LDP session impacts the associated VPLS or VLL sessions. Resetting an LDP session which is not in an operational state has no impact.

When the LDP session is not found corresponding to the specified *peer-ip-addr* and, if applicable, *label-space*, a warning message is displayed.

When an LDP session is not in operational state, resetting it has no impact.

When the **all** option is specified, all LDP sessions on the Brocade device is reset, including the targeted LDP sessions.

Examples

The following example clears both the link and targeted LDP session with neighbor 10.234.123.64 because the *label_space* optional parameter has not been specified.

```
device# clear mpls ldp neighbor 10.234.123.64
device#
```

clear mpls ldp statistics

Clears the LDP packet statistics displayed by the **show mpls ldp statistics** command.

Syntax

clear mpls ldp statistics

Modes

Privileged EXEC mode

Usage Guidelines

This command clears packet statistics including packet types and packet errors.

Examples

The following example clears the LDP packet statistics.

```
device# clear mpls ldp statistics
```

clear mpls rsvp statistics session

Clears RSVP session statistics.

Syntax

clear mpls rsvp statistics session { [[**destination** *ip_addr*]] [**source** *source_ip*] [**tunnel-id** *tunnel_id* **lsp-id** *lsp_id*]] | { **name** *session_name*] } | { **p2mp p2mp-id** [*ip_addr* | *dec*] } [**source** *source_ip*] [**tunnel-id** *tunnel_id lsp_id*]

Parameters

destination *ip_addr*

Defines the destination IP address.

source *source_ip*

Defines the source IP address.

tunnel *tunnel _id*

Defines the tunnel by decimal number 1 - 65535.

lsp-id *lsp_id*

Defines the LSP by decimal number 1 - 65535.

name *session_name*

Clears the session by name.

p2mp p2mp-id

Clears the point to multipoint sessions.

ip_addr

Specifies the P2MP identifier as an IP address

dec

Specifies the P2MP identifier as a decimal.

Modes

Privileged EXEC mode.

Usage Guidelines

This command operates in all modes.

Examples

The following example clears the RSVP session statistics for the lsp_test session.

```
device(config)# clear mpls rsvp statistics session
device(config)# clear mpls rsvp statistics session destination 11.11.11.11
device(config)# clear mpls rsvp statistics session destination 11.11.11.11 source 14.14.14.14
device(config)# clear mpls rsvp statistics session destination 11.11.11.11 source 14.14.14.14 tunnel-id
10
device(config)# clear mpls rsvp statistics session name lsp_test
device(config)# clear mpls rsvp statistics session p2mp p2mp-id 1.1.1.1 source 1.1.1.1 tunnel-id 1
```

History

Release version	Command history
5.9.00	This command was modified to provide the same statistics that are available at the global and interface level at the per-session level.

clear mpls statistics

Clears MPLS statistics.

clear mpls statistics 6pe [*slot/port* | **vrf**]

clear mpls statistics bypass-lsp *lsp_name*

clear mpls statistics label [*num* | *slot***/***port*]

clear mpls statistics ldp [**transit** | **tunnel**]

clear mpls statistics lsp *lsp_name*

clear mpls statistics oam

clear mpls statistics rsvp [**neighbor** | **session**]

clear mpls statistics tunnel *num*

clear mpls statistics vll [*vll_id* | *vll_name*]

clear mpls statistics vll-local [*vll_local_id* | *vll_local_name*]

clear mpls statistics vpls [*vpls_id* | *vpls_name*]

clear mpls statistics vrf *vrf_name*

Parameters

6pe

Clears 6pe statistics.

slot **/***port*

Interface slot and port number.

vrf

Clears IPv6 VRF statistics.

bypass-lsp

Clears statistics for bypass LSPs.

lsp_name

Name of targeted LSP.

label

Clears in-label statistics.

num

In-label.

slot/port

Interface number.

ldp

Clears ingress tunnel accounting for LDP signaled LSP.

transit

Clears transit traffic statistics for LDP.

tunnel
Clears ingress tunnel accounting for LDP created tunnels.

lsp
Clears ingress tunnel accounting for RSVP signaled LSP.

lsp_name
Name of targeted LSP.

oam
Clears OAM statistics.

rsvp
Clears transit statistics for RSVP signaled LSP.

neighbor
Clears statistics for RSVP neighbor.

session
Clears transit statistics for RSVP sessions.

tunnel
Clears MPLS tunnel statistics.

num
Tunnel interface index.

vll
Clears VLL statistics.

vll_id
VLL identifier.

vll_name
Name of VLL.

vll-local
Clears VLL local statistics.

local_vll_id
Local VLL identifier.

local_vll_name
Name of local VLL.

vpls
Clears VPLS statistics.

vpls_id
VPLS identifier.

vpls_name
Name of VPLS.

vrf
Clears VRF statistics.

vrf_name
Name of VRF.

Modes

Privileged EXEC mode.

Examples

The following example clears bypass LSPs statistics:

```
device# clear mpls statistics bypass-lsp
Cleared statistics of bypass LSPs
```

History

Release version	Command history
5.7.00	This command was modified to include the **bypass-lsp** keyword.

clear mvrp statistics

Clears MVRP port statistics.

Syntax

clear mvrp statistics [**ethernet** *slot*/*port*]

Parameters

ethernet *slot*/*port*

Clears MVRP statistics for the specified interface.

Modes

Privileged EXEC mode

Examples

The following example clears MVRP statistics for all ports.

```
device# clear mvrp statistics
```

The following example clears MVRP statistics for a specific port.

```
device# clear mvrp statistics ethernet 1/1
```

clear openflow

Clears flows from the flow table.

Syntax

clear openflow { **flowid** *flow-id* | **all** }

Parameters

flowid *flow-id*

Clears the given flow ID that you want to delete from the flow table.

all

Deletes all flows from the flow table.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

When an OpenFlow rule or all flows in the flow table need to be deleted you can use the **clear openflow** command with the **all** option. To delete a single OpenFlow rule based on a flow-id, use the **clear openflow** command with the **flowid** *flow-id* options.

Examples

The following example clears the flow with an ID of 6.

```
device# clear openflow flowid 6
```

The following example clears all flows in the flow table.

```
device# clear openflow all
```

History

Release	Command History
NI05.5.00c	This command was modified to delete a single flow on a specified flow-id or all flow deletion in the flow table.

clear pki counters

Clears the Public Key Infrastructure (PKI) counters for a certificate authority (CA).

Syntax

clear pki counters

Modes

PKI trustpoint configuration mode.

Examples

The following example clears the PKI counters for the CA.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# clear pki counters
```

History

Release version	Command history
5.9.00	This command was introduced.

clear pki crl

Removes the certificate revocation list (CRL) database for a specific trustpoint name.

Syntax

clear pki crl *trustpoint name*

Parameters

trustpoint name

Specifies the trustpoint name whose CRL database has to be removed.

Modes

PKI trustpoint configuration mode.

Examples

The following example removes the CRL database for the specified trustpoint name.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# clear pki crl Trustpoint1
```

History

Release version	Command history
5.9.00	This command was introduced.

clear rate-limit counters bum-drop

Clears the accounting information for the Broadcast, Unicast, Multicast (BUM) traffic rate limit.

Syntax

clear rate-limit counters bum-drop [*portid*] [*vlanid*]

clear rate-limit counters bum-drop [**shutdown**] [*portid*] *slot*/*port* [**all**] [*vlan-id*] [*vlan*]]

Parameters

portid

Optionally clears the accounting information for BUM rate-limiting for the specified port.

vlanid

Optionally clears the accounting information for BUM rate-limiting for the specified VLAN.

Modes

Privileged EXEC configuration mode

Usage Guidelines

This command is used to clear rate-limiting accounting information for BUM traffic and, optionally, for specified interfaces or VLANs.

Examples

The following example clears the BUM rate-limiting information for VLAN 2.

```
device# clear rate-limit counters bum-drop vlan2
```

History

Release version	Command history
5.7.00	This command was introduced.

clear rate-limit counters ip-option-pkt-to-cpu

Clears the rate-limit counters for IPv4 option packets.

Syntax

clear rate-limit counters ip-option-pkt-to-cpu

Modes

This command operates in all mode.

Examples

The following example shows how to clear the rate-limit counters for IPv4 option packets.

```
Brocade# clear rate-limit counters ip-option-pkt-to-cpu
```

History

Release version	Command history
Multi-Service IronWare Release 5.8.00	This command was introduced.

clear rate-limit counters ipv6-hoplimit-expired-to-cpu

Clears the rate-limit counters for IPv6 hoplimit-expired-to-cpu packets.

Syntax

clear rate-limit counters ipv6-hoplimit-expired-to-cpu

Modes

This command operates in all mode.

Examples

The following example shows how to clear the rate-limit counters for hoplimit-expired-to-cpu packets.

```
Brocade# clear rate-limit counters ipv6-hoplimit-expired-to-cpu
```

History

Release version	Command history
Multi-Service IronWare Release 5.8.00	This command was introduced.

clear rate-limit counters ip-ttl-expired-to-cpu

Clears the rate-limit counters for IPv4 ttl-expired-to-cpu packets.

Syntax

clear rate-limit counters ip-ttl-expired-to-cpu

Modes

This command operates in all mode.

Examples

The following example shows how to clear the rate-limit counters for ip-ttl-expired-to-cpu.

```
Brocade# clear rate-limit counters ip-ttl-expired-to-cpu
```

History

Release version	Command history
Multi-Service IronWare Release 5.8.00	This command was introduced.

clear statistics openflow

Clears OpenFlow statistics.

Syntax

clear statistics openflow { **group** | **meter** | **controller** }

Parameters

group

Clears statistics for all groups.

meter

Clears statistics for all meters.

controller

Clears statistics for all controllers.

Modes

EXEC and Privileged EXEC mode

Global configuration mode

Usage Guidelines

This command can be entered in three configuration modes as shown in the examples below.

Examples

The following example, entered in User EXEC mode, clears statistics for all groups in User EXEC mode.

```
device> clear statistics openflow group
```

The following example, entered in Privileged EXEC mode, clears statistics for all meters in Privileged EXEC mode.

```
device> enable
device# clear statistics openflow meter
```

The following examples, entered in global configuration mode, clears statistics for all controllers.

```
device# configure terminal
device(config) # clear statistics openflow controller
```

History

Release	Command History
NI05.7.00	This command was introduced.

client-interfaces sync_ccep_early

Adds a time delay before the Cluster Client Edge Port (CCEP) goes to the forwarding state.

Syntax

client-interfaces sync_ccep_early lacp-delay *value*

no client-interfaces sync_ccep_early lacp-delay *value*

Command Default

There is no time delay set when Link Aggregation Control Protocol (LACP) is in the blocked state.

Parameters

lacp-delay

Configures a time delay for the LACP blocked state.

value

Specifies the time delay value in seconds. The valid values are from 3 through 10 seconds. The default value is 3 seconds.

Modes

MCT cluster configuration mode

Usage Guidelines

The command enables faster synchronization of the CCEP *up* or *down* state to the MCT node.

NOTE

Configure this command only when required because there may be high broadcast, unknown unicast and multicast (BUM) traffic drops due to this configuration.

The **no** form of the command removes the predefined time delay for the LACP blocked state.

Examples

The following example sets a time delay of 8 seconds berfore the CCEP goes to the forwarding state for the MCT cluster "abc".

```
device(config)# cluster abc 1
device(config-cluster-abc)# client-interfaces sync_ccep_early lacp-delay 8
```

History

Release version	Command history
6.0.0	This command was introduced.

cluster-client-static-mac-move

Enables the static MAC address movement from the local Cluster Client Edge Port (CCEP) to the Inter-Chassis Link (ICL) port in the MAC cluster and vice versa.

Syntax

cluster-client-static-mac-move

no cluster-client-static-mac-move

Modes

MCT cluster configuration mode

Usage Guidelines

This command must be configured in both the MCT peers but the static MAC address under the VLAN must be configured on any one of the MCT peers.

The **no** form of the command disables the static MAC address movement from the local CCEP to the ICL port.

Examples

The following example enables the static MAC address movement from the local CCEP to the ICL port (and vice versa) in the MAC cluster named "brocade" with the cluster ID set as 1.

```
device(config)# cluster brocade 1
device(config-cluster-brocade)# cluster-client-static-mac-move
```

History

Release version	Command history
5.9.00	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.

Examples

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

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

copy

Copies a file from a source device to a destination server (usually remote) or from a server (source) to a Brocade device (destination). This command can also be used to upload or download a configuration file. Each syntax instance is slightly different for the various operations.

Syntax

copy *source protocol* { *ipv4-address* | *ipv6-address* } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename device-filename*

copy *protocol destination* { *ipv4-address* | *ipv6-address* } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename device-filename*

copy *config-file protocol* { *ipv4-address* | *ipv6-address* } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

copy *protocol config-file* { *ipv4-address* | *ipv6-address* } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

source

Specifies the location of the file on the source device to be copied to the server. Can be one of the following: **flash**, **scp**, **slot1**, or **slot2** depending on the device. CES and CER devices support only the flash option.

protocol

Specifies the protocol to be used. Can be one of the following: **flash**, **http**, **https**, or **scp**.

destination

Specifies the location on the destination device where the file is to be copied from the server. Can be one of the following: **flash**, **scp**, **slot1**, **slot2**, depending on the device. CES and CER devices support only the **flash** option.

ipv4-address

Specifies the IPv4 address of the server.

ipv6-address

Specifies the IPv6 address of the server.

remote-filename

Specifies the name of the file to be used on the remote server. You can specify up to 127 characters for the file name.

device-filename

Specifies the name of the file to be used on the local device. Certain filenames are reserved and the system will not allow you to use them.

config-file

Specifies the configuration file to be used. Can be either **running-config** or **startup-config**.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for *username* and *password* when you execute this command. The maximum length is 48 characters for each.

Please note that each syntax instance is different and is used to perform the following actions:

- Upload a copy of a file from a Brocade device (source) using a specified protocol to a server (destination) using the first syntax
- Download a copy of a file from a server (destination) using a specified protocol to a Brocade device (source) using the second syntax
- Upload a configuration file using the third syntax
- Download a configuration file using the fourth syntax

NOTE
When downloading a file to flash, the destination filename cannot be same as any of the reserved file names in flash. CLI will throw the following error when destination filename is any of the reserved file name: Error: Destination file name(%s) cannot be same as any of the reserved file names in flash.

Examples

The following example uploads a copy of an OS image file from the primary flash memory on a device to an SCP server with the IP address of 172.26.51.180:

```
device# copy scp slot1 172.26.51.180 public-key dsa image-filename primary
```

The following example downloads a copy of an file from an SCP server to a Brocade device with the IP address of 10.20.99.146

```
device# copy flash scp 10.20.99.146 ~/xmr05800.bin primary
```

The following example uploads a copy of the image file “startup-config” from the primary flash memory on a device to a file named “startup-config-srv.txt” on an HTTP server with the IP address of 172.26.51.180:

```
device# copy flash http 172.26.51.180 startup-config-srv.txt startup-config
```

The following example downloads a copy of the image file “startup-config-srv.txt” from the HTTP server with the IP address of 172.26.51.180 to a “startup-config” file on slot2 of the device.

NOTE
When downloading, the system will not allow you to use certain filenames as a destination (target) filename.

```
device# copy http slot2 172.26.51.180 startup-config-srv.txt startup-config-dev.txt
```

copy tftp license

Copies the license file from the TFTP server to the license database of the Brocade device.

Syntax

copy tftp license { *ip_address* | *ipv6_address* } *license_filename_on_host*

Command Default

By default, the command is not enabled.

Parameters

ip_address
Specifies the address of the IPv4 TFTP server.

ipv6_address
Specifies the address of the IPv6 TFTP server.

license_filename_on_host
Specifies the filename of the license file.

Modes

Privileged EXEC level.

Usage Guidelines

To remove a license file, use the **license delete** command.

If you attempt to download the same license twice on the device, the following error message is displayed on the console.

Can't add the license string - 93 (DUPLICATE_LICENSE)

Examples

The following example copies the license file from the TFTP server to the license database of the Brocade device.

```
device# copy tftp license 10.1.1.1 lic.xml
```

History

Release version	Command history
07.1.00	This command was introduced.
05.0.00	This command was introduced.

copy-received-cos

Classifies and prioritizes the management traffic for QoS.

Syntax

copy-received-cos protocol

Parameters

SSH

Specifies the SSH protocol.

Telnet

Specifies the Telnet protocol.

Modes

History

Release version	Command history
5.7.00	This command was introduced.

common-name

Specifies the common name parameter for the Public Key Infrastructure (PKI) entity.

Syntax

common-name *name*

Parameters

name

Specifies the common name parameter for the PKI entity.

Modes

PKI entity configuration mode

Examples

The following example specifies the common name parameter for the PKI entity.

```
device(config)# pki entity brocade_entity
device(config-pki-entity-brocade_entity)# common-name brocade_e
```

History

Release version	Command history
05.8.00	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

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

Examples

This example configures the device to compare MEDs:

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

compare-routerid

Enables comparison of device IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

Syntax

compare-routerid

no compare-routerid

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

This example configures the device always to compare device IDs.

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

confederation identifier

Configures a BGP confederation identifier.

Syntax

confederation identifier *autonomous-system number*

no confederation identifier

Command Default

No BGP confederation identifier is identified.

Parameters

autonomous-system number

Specifies an autonomous system number (ASN). The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove a BGP confederation identifier.

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

Examples

This example specifies that confederation 65220 belongs to autonomous system 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# local-as 65220
device(config-bgp)# confederation identifier 100
```

confederation peers

Configures subautonomous systems to belong to a single confederation.

Syntax

confederation peers *autonomous-system number* [*...autonomous-system number*]

no confederation peers

Command Default

No BGP peers are configured to be members of a BGP confederation.

Parameters

autonomous-system number

Autonomous system (AS) numbers for BGP peers that will belong to the confederation. The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove an autonomous system from the confederation.

Examples

This 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)# local-as 65020
device(config-bgp)# confederation identifier 100
device(config-bgp)# confederation peers 65520 65521 65522
```

cos

Configures the a Class of Service (CoS) priority value for all packets traveling through the LSP.

Syntax

cos *number*

no cos *number*

Parameters

number

Specifies the CoS priority value. Enter a number from 0 to 7. The lowest priority is 0, the default value. The highest priority is 7.

Modes

MPLS LSP configuration mode

Usage Guidelines

The 3-bit EXP field in the MPLS header defines a CoS value for packets traveling through the LSP. When you set the CoS value, it is applied to the EXP field in the MPLS header of all packets entering this LSP. Then, all packets traveling through an LSP have the same priority as they travel the MPLS domain.

The MPLS CoS value determines the priority within an MPLS domain only. When the label is popped, the CoS value in the MPLS header is discarded and it is not copied back to the IP ToS field.

Use the **no** form of the command to remove the configured setting.

Examples

The following example configures the CoS priority of 7 to all packets traveling through the tunnel4 LSP.

```
device(config-mpls)# lsp tunnel4
device(config-mpls-lsp-tunnel4)# cos 7
```

country-name

Configures the country code for the Public Key Infrastructure (PKI) entity.

Syntax

country-name *name*

Parameters

name

Specifies the country code for the PKI entity.

Modes

PKI entity configuration mode

Usage Guidelines

The country code is specified as a standard two-character code for a country. For example, IN can be the country code for India and US for United States of America.

Examples

The following example configures the India country code for the PKI entity.

```
device(config)# pki entity brocade_entity
device(config-pki-entity-brocade_entity)# country-name IN
```

History

Release version	Command history
5.8.00	This command was introduced.

crl-query

Sets the certificate revocation list (CRL) URL name if the revocation check is configured as CRL in the device.

Syntax

crl-query *URL name*

no crl-query *URL name*

Parameters

URL name

The CRL URL name.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The **no** form of the command removes the specified CRL URL name.

Examples

The following example specifies the CRL URL name as provided.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# crl-query http://WIN-HJ98AK136A0.englab.brocade.com/CertEnroll/
englab-WIN-HJ98AK136A0-CA-7.crl
```

History

Release version	Command history
5.9.00	This command was introduced.

crl-update-time

Sets the certificate revocation list (CRL) update period for a certificate.

Syntax

crl-update-time *hours*

no crl-update-time *hours*

Command Default

The CRL update period depends on the next update field in the CRL file.

Parameters

hours

The CRL update period value in hours. Valid values range from 1 through 1000 hours.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The **no** form of the command removes the specified CRL update time.

Examples

The following example specifies the CRL update time as 10 hours.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# crl-update-time 10
```

History

Release version	Command history
5.9.00	This command was introduced.

crypto key generate

Generates a cryptographic key pair on a device.

Syntax

crypto key generate dsa

crypto key generate ec label *name*[**size** *key-size*]

crypto key generate rsa modulus *key-size*

Command Default

A cryptographic key pair is not present on the device.

Parameters

dsa

Specifies the generation of a Digital Signature Algorithm (DSA) key pair.

ec

Specifies the generation of an Elliptic Curve (EC) key pair.

label *name*

Specifies a label name for the EC key pair in ASCII-string format. The maximum string length is 16 characters.

size *key-size*

(Optional) Specifies the size of the EC key pair in bits. Possible values are 256 and 384. A 384-bit key provides the highest level of security. The default key size is 384 bits.

rsa

Specifies the generation of a Rivest, Shamir and Adelman (RSA) key pair.

modulus *key-size*

Specifies the size of the RSA key pair in bits. Possible values are 1024 and 2048. In Federal Information Processing Standard (FIPS) mode a 2048-bit RSA key size is required. In non-FIPS mode, either a 1024-bit or 2048-bit key may be specified.

Modes

Global configuration mode

Usage Guidelines

After generating an EC key pair, you can specify using it for enrollment with a certification authority (CA) by using the **eckeypair** command in Public Key Infrastructure (PKI) trustpoint configuration mode.

Examples

The following examples shows how to generate a 384-bit EC key pair and specify using the label ec_key1 for the key pair.

```
device(config)# crypto key generate ec label ec_key1 size 384
```

History

Release version	Command history
NI 5.9.00	This command was modified to add the **ec** option.
NI 5.9.00a	This command was modified to add the **size** option when generating an Elliptic Curve (EC) key pair.

crypto key zeroize

Deletes cryptographic keys on a device.

Syntax

crypto key zeroize [{**dsa** | **rsa** | **ec label** *name* }]

Parameters

dsa

Specifies deleting the Digital Signature Algorithm (DSA) key pair from the device.

rsa

Specifies deleting the Rivest, Shamir and Adelman (RSA) key pair from the device.

ec label*name*

Specifies the label of an Elliptic Curve (EC) key pair to delete from the device.

Modes

Global configuration mode

Examples

The following example shows how to delete all cryptographic key pairs on a device.

```
device(config)# crypto key zeroize
```

The following example shows how to delete a specific Elliptic Curve (EC) key pair labeled ec_key1.

```
device(config)# crypto key zeroize ec label ec_key1
```

History

Release version	Command history
NI 5.9.00	This command was modified to add the **ec** option.

csnp-interval

Configures the Complete Sequence Number PDU (CSNP) interval.

Syntax

csnp-interval *secs*

no csnp-interval

Command Default

The default CSNP interval is 10 seconds.

Parameters

secs

Specifies the interval in seconds. Valid values range from 0 through 65535 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

The interval configured on the device applies to both Level 1 and Level 2 CSNPs and Partial Sequence Number PDUs (PSNPs).

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

Examples

The following example configures a CSNP interval of 25 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# csnp-interval 25
```

cspf-computation-mode

Configures the IS-IS ignore overload bit.

Syntax

cspf-computation-mode [**ignore-overload-bit** | **use-bypass-liberal** | **use-bypass-metric** | **use-igp-metric** | **use-te-metric**]

no cspf-computation-mode [**ignore-overload-bit** | **use-bypass-liberal** | **use-bypass-metric** | **use-igp-metric** | **use-te-metric**]

Command Default

By default, this command is disabled.

Parameters

ignore-overload-bit
Ignores the overload bit during CSPF computation.

use-bypass-liberal
Uses the liberal mode for CSPF facility backup computation.

use-bypass-metric
Uses the bypass LSPs path for cost for selection between bypass LSPs.

use-igp-metric
Uses the IGP metric of the link for CSPF computation.

use-te-metric
Uses the TE metric of the link for CSPF computation.

Modes

MPLS policy configuration mode

Usage Guidelines

The **no** form of the command allows CSPF to reject the path transiting through and overloaded router from the ingress.

Configuring this command will indicate that all the future CSPF calculations through an overloaded transit router are not rejected.

Because the command is at the global level, it will affect all the LSPs.

Examples

The following example configures the software to ignore the overload bit during CSPF computation. The output of the **show mpls config** command verifies the configuration.

```
device(config-mpls-policy)# cspf-computation-mode ignore-overload-bit
device(config-mpls-policy)#show mpls config
router mpls
 policy
  traffic-eng isis level-1
  handle-isis-neighbor-down
  cspf-computation-mode ignore-overload-bit
```

History

Release version	Command history
5.8.00	This command was introduced.

cspf-computation-mode (LSP level)

Configures the CSPF computation mode for RSVP LSPs.

Syntax

cspf-computation-mode [**use-igp-metric** | **use-te-metric**]

no cspf-computation-mode [**use-igp-metric** | **use-te-metric**]

Command Default

By default, LSP uses the CSPF computation mode from the global configuration at MPLS policy level.

Parameters

use-igp-metric

Uses the IGP metric of the link for CSPF computation.

use-te-metric

Uses the TE metric of the link for CSPF computation

Modes

Primary, secondary, and at static bypass LSP context level under the router MPLS mode.

Usage Guidelines

The **cspf-computation-mode** command configures the computation mode for CSPF to use TE-metric or IGP-metric at primary, secondary, and static bypass LSP levels by overriding global LSP configuration.

The **no** version of this command will set the CSPF computation to use the global configuration from router MPLS policy level.

Examples

The following example explains configuration of CSPF computation mode to use TE-metric or IGP-metric at LSP level.

```
device(config)# router mpls
device(config-mpls)# lsp test
device(config-mpls-lsp-test)# cspf-computation-mode ?
    use-igp-metric         use IGP metric of the link for CSPF computation
    use-te-metric             use TE metric of the link for CSPF computation

device(config-mpls-lsp-test)# cspf-computation-mode use-igp-metric
device(config-mpls-policy)# no cspf-computation-mode use-te-metric
Error:CSPF computation is configured to use igp-metric

device(config-mpls-policy)# no cspf-computation-mode use-igp-metric
```

History

Release version	Command history
5.6.00	This command was introduced.

database-overflow-interval (OSPFv2)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

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

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This command specifies how long a device that has entered the OverflowState waits before resuming normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the device lapses back into OverflowState. If the configured value of the database overflow interval is zero, then the device never leaves the database overflow condition.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the device enters OverflowState. In this state, the device flushes all non-default AS-external-LSAs that the device had originated. The devie also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

The **no** form of the command disables the overflow interval configuration.

Examples

The following example configures a database-overflow interval of 60 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# database-overflow-interval 60
```

database-overflow-interval (OSPFv3)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

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

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds (24 hours).

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

This command specifies how long after a router that has entered the OverflowState before it can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

If the configured value of the database overflow interval is 0, then the device never leaves the database overflow condition.

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-ospf6-router)# database-overflow-interval 120
```

dead-interval

Configures the interval for which a Virtual Router Redundancy Protocol (VRRP) backup router waits for a hello message from the VRRP master router before determining that the master is offline. When backup routers determine that the master is offline, the backup router with the highest priority becomes the new VRRP master router.

Syntax

dead-interval [**msec**] *interval*

no dead-interval [**msec**] *interval*

Command Default

The default dead interval is internally derived from the hello interval. It is equal to 3 times the hello interval plus the skew time, where the skew time is equal to (256 minus the priority) divided by 256.

Parameters

msec *interval*

Sets the interval, in milliseconds, for which a VRRP backup router waits for a hello message from the VRRP master router before determining that the master is offline. Valid values range from 100 through 84000. The default value is 1000. VRRP-E does not support the dead interval in milliseconds.

interval

Sets the interval, in seconds, for which a VRRP backup router waits for a hello message from the VRRP master router before determining that the master is offline. Valid values range from 1 through 84. The default value is 1.

Modes

VRID interface configuration mode

Usage Guidelines

By default, the dead interval is internally derived from the hello interval. It is equal to 3 times the hello interval plus the skew time, where the skew time is equal to (256 minus the priority) divided by 256. Generally, if you change the hello interval on the VRRP master device using the **hello-interval** command, you should also change the dead interval on the VRRP backup devices using the **dead-interval** command.

A VRRP master router periodically sends hello messages to the backup routers. The backup routers use the hello messages as verification that the master is still online. If the backup routers stop receiving the hello messages for the period of time specified by the dead interval, the backup routers determine that the master router is offline. At that point, the backup router with the highest priority becomes the new master router.

The **dead-interval** command is configured only on VRRP backup routers and is supported by VRRP and VRRP-E.

The **no** form resets the dead interval to its default value of 1000 milliseconds (1 second).

NOTE

VRRP-E does not support the hello message interval in milliseconds.

Examples

The following example sets a waiting period of 25000 milliseconds before a VRRP backup router determines that a VRRP master router is offline.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# backup priority 40 track-priority 10
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.99
device(config-if-e1000-1/6-vrid-1)# dead-interval msec 25000
device(config-if-e1000-1/6-vrid-1)# activate
```

The following example sets a waiting period of 25 seconds before a VRRP-E backup router determines that a VRRP master router is offline.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(conf-if-e1000-1/5)# ip address 10.53.5.3/24
device(conf-if-e1000-1/5)# ip vrrp-extended vrid 2
device(conf-if-e1000-1/5-vrid-2)# backup priority 50 track-priority 10
device(conf-if-e1000-1/5-vrid-2)# ip-address 10.53.5.1
device(conf-if-e1000-1/5-vrid-2)# dead-interval 25
device(conf-if-e1000-1/5-vrid-2)# activate
```

dead-interval (vsrp)

Configures the number of seconds a backup waits for a Hello message from the master before determining that the master is dead.

Syntax

dead-interval *number*

no dead-interval *number*

Command Default

The default time interval for the backup to wait for the Hello message from the master is 3 units of 100 ms (300 milliseconds).

Parameters

number

Specifies the time interval for which the backup waits for the Hello message from the master. The time interval range is from 3 through 84 units of 100 milliseconds.

Modes

VSRP VRID configuration mode

Usage Guidelines

The **no** form of the command resets the time interval to the default value.

Examples

The following example shows how to change the dead interval.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vsrp-1)# dead-interval 30
```

default-information-originate (IS-IS)

Generates a default route into an Intermediate System-to-Intermediate System (IS-IS) routing domain.

Syntax

default-information-originate [**route-map** *name*]

no default-information-originate [**route-map** *name*]

Command Default

Disabled.

Parameters

route-map *name*

Specifies that the default route is generated if the route map is satisfied. The route map name can be from 1 through 63 characters in length.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

The **no** form of the command disables default route origination.

Examples

The following example generates a default external route into an IS-IS domain.

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

The following example generates a default external route into an IS-IS domain if the route map “myroutemap” is satisfied

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-isis-router-ipv6u)# default-information-originate route-map myroutemap
```

default-information-originate (OSPFv2)

Controls distribution of default information to an OSPFv2 device.

Syntax

default-information-originate [**always**] [**metric** *metric*] [**metric-type** { **type1** | **type2** }] [**route-map** *name*]

no default-information-originate

Command Default

The default route is not advertised into the OSPFv2 domain.

Parameters

always

Always advertises the default route. If the route table manager does not have a default route, the router advertises the route as pointing to itself.

metric *metric*

specifies the cost for reaching the rest of the world through this route. If you omit this parameter and do not specify a value using the *default-metric* router configuration command, a default metric value of 1 is used. Valid values range from 1 through 65535. The default is 10.

metric-type

Specifies how the cost of a neighbor metric is determined. The default is **type1**. However, this default can be changed with the **metric-type** command.

type1

Type 1 external route.

type2

Type 1 external route,

route-map *name*

Specifies that the default route is generated if the route map is satisfied. This parameter overrides other options. If the **set metric** and **set metric-type** commands are specified in the route-map, the command-line values of metric and metric-type if specified, are “ignored” for clarification.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the route table manager (RTM),whether static or learned from another protocol, to its neighbors.

The corresponding route-map should be created before configuring the **route-map** option, along with the **default-information-originate** command. If the corresponding route-map is not created beforehand, an error message is displayed stating that the route-map must be created.

The route-map option cannot be used with a non-default address in the match conditions. The default route LSA is not generated if a default route is not present in the routing table and a **match ip address** condition for an existing non-default route is configured in the route-map. The **match ip address** command in the route-map is a no-op operation for the default information originate command.

A device does not inject the default route into an NSSA by default and this command does not cause the device to inject the default route into the NSSA. To inject the default route into an NSSA, use the **area nssa 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-ospf-router)# default-information-originate metric 30 metric-type type1
```

default-information-originate (OSPFv3)

Controls distribution of default information to an OSPFv3 device.

Syntax

default-information-originate [**always**] [**metric** *metric*] [**metric-type** { **type1** | **type2** }]

no default-information-originate

Command Default

The default route is not advertised into the OSPFv3 domain.

Parameters

always

Always advertises the default route. If the route table manager (RTM) does not have a default route, the router advertises the route as pointing to itself.

metric *metric*

Used for generating the default route, this parameter specifies the cost for reaching the rest of the world through this route. If you omit this parameter, the value of the **default-metric** command is used for the route. Valid values range from 1 through 65535.

metric-type

Specifies the external link type associated with the default route advertised into the OSPF routing domain.

type1

The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.
If you do not use this option, the default redistribution metric type is used for the route type.

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.

If you specify a metric and metric type, the values are used even if you do not use the always option.

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-ospf6-router)# default-information-originate metric 20 metric-type type2
```

default-link-metric

Configures the metric value globally on all active IS-IS interfaces for the configured address family.

Syntax

default-link-metric *value* [**level-1** | **level-2**]

no default-link-metric *value* [**level-1** | **level-2**]

Command Default

Disabled.

Parameters

value

Specifies the default-link-metric value in metric style and configurable range. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default is 10.

level-1

Specifies the default-link-metric parameter as either level 1.

level-2

Specifies the default-link-metric parameter as either level 2.

Modes

ISIS address-family IPv4 unicast configuration mode

ISIS address-family IPv6 unicast configuration mode

Usage Guidelines

Use this command to change the metric value globally on all active IS-IS interfaces for the configured address family. This command is useful when you have a common IS-IS metric value on all IS-IS interfaces, other than the default metric value of 10. This command is not applicable to MPLS IS-IS shortcuts and tunnel interfaces.

If you change the metric style configuration, the default-link-metric value also changes. The new default-link-metric value is equal to the minimum of the configured value, and the maximum value supported by the new metric style. For example, if the metric style changes from a wide metric to a narrow metric, and the default-link-metric value is greater than 63, the default-link-metric value changes to 63 because it is the maximum value supported in the narrow metric style. When the metric style changes from a narrow metric to a wide metric, there is no change to the default-link-metric value.

If the IS-IS routing parameter is not configured, the default-link-metric value is applied to both level-1 and level-2.

You can change the metric value for a specific interface using the **isis metric** command or the **isis ipv6** command. The **isis metric** command configuration takes precedence over the **default-link metric** *value* command configuration.

During switchover or hitless upgrade, the IS-IS default link metric configuration is not affected. Backward compatibility is not supported.

The **no** form of the command resets the metric value to the default value 10.

NOTE
The **default-link metric** *value* command is supported on the Brocade NetIron XMR Series, the Brocade MLX Series, and the Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

Examples

The following example configures the IS-IS default link metric value to 30 for the IPv4 address family. The default-link-metric value of 30 is applied to both Level 1 and Level 2.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-isis-router-ipv4u)# default-link-metric 30
```

The following example configures the IS-IS default link metric value to 30 for Level 1, and the IS-IS default link metric value of 40 to level-2.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family-ipv4 unicast
device(config-isis-router-ipv4u)# default-link-metric 30 level-1
device(config-isis-router-ipv4u)# default-link-metric 40 level-2
```

Use the **show isis** command to display the configuration for the IS-IS default link metric value.

```
device(config)# show isis
…..
Default redistribution metric: 0
Default link metric for level-1: 33 (conf)/ 33 (adv)
Default link metric for level-2: 5 (conf)/ 5 (adv)
Protocol Routes redistributed into IS-IS:
…..
```

History

Release version	Command history
5.7.00	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

Command Default

The default local preference is 100.

Parameters

num

Local preference value. Range is from 0 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

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

Use this command to change the local preference value. Local preference indicates a degree of preference for a route relative to that of other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message.

Examples

This example sets the local preference value to 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# default-local-preference 200
```

default-metric (IS-IS)

Sets the default redistribution metric value for the Intermediate System-to-Intermediate System (IS-IS) routing protocol.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 0.

Parameters

value

Specifies the default metric value. Valid values range from 0 through 65535. The default is 0.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

The **no** form of the command resets the default metric value to the default value of 0.

Examples

The following example sets the default metric value to 20 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-isis-router-ipv4u)# default-metric 20
```

The following example sets the default metric value to 40 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-isis-router-ipv6u)# default-metric 40
```

default-metric (OSPF)

Sets the default metric value for the OSPFv2 or OSPFv3 routing protocol.

Syntax

default-metric *metric*

no default-metric

Command Default

The default metric value for the OSPFv2 or OSPFv3 routing protocol is 10.

Parameters

metric

OSPF routing protocol metric value. Valid values range from 1 through 65535.

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)# router ospf
device(config-ospf-router)# default-metric 20
```

default-passive-interface

Marks all OSPFv2 and OSPFv3 interfaces passive by default.

Syntax

default-passive-interface

no default-passive-interface

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

When you configure the interfaces as passive, the interfaces drop all the OSPFv2 and OSPFv3 control packets.

You can use the **ip ospf active** and **ip ospf passive** commands in interface subconfiguration mode to change active/passive state on specific OSPFv2 interfaces. You can use the **ipv6 ospf active** and **ipv6 ospf passive** commands in interface subconfiguration mode to change the active and passive state on specific OSPFv3 interfaces.

The **no** form of the command disables the passive state.

Examples

The following example marks all OSPFv2 interfaces as passive.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# default-passive-interface
```

The following example marks all OSPFv3 interfaces as passive for VRF “red”.

```
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ospf6-router-vrf-red)# default-passive-interface
```

delete-certificate

Deletes all the trustpoint certificates or a specific certificate associated with a trustpoint.

Syntax

delete-certificate [*certificate-serial-number*]

Parameters

certificate-serial-number

Specifies the serial number of the certificate.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

When the local certificate is deleted, the existing established IKEv2 SA are not affected but any new IKEv2 SA establishment is not allowed if x509v3 certificate is needed for authentication.

NOTE

This command is applicable only for certificates downloaded from CA server.

Examples

The following example deletes a specific trustpoint certificate.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# delete-certificate fe:75:d1:a3:bc:56:28:8e
```

History

Release version	Command history
5.8.00	This command was introduced.

deny (IPv6 ACL rules)

Inserts deny filtering rules into IPv6 ACLs. These rules deny traffic according to source and destination addresses, port protocol, and other IPv6 frame content.

Syntax

Use the following syntax to define a TCP rule:

deny [**enable-accounting**] [**vlan** *vlan-id*] **tcp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**established**] [**syn**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to define an ICMP rule:

deny [**enable-accounting**] [**vlan** *vlan-id*] **icmp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*icmp-parameters*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to define an SCTP or UDP rule:

deny [**enable-accounting**] [**vlan** *vlan-id*] { **sctp** | **udp** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to define an AHP, ESP, or IPv6 rule:

deny [**enable-accounting**] [**vlan** *vlan-id*] { **ahp** | **esp** | **ipv6** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to delete a rule, specifying the sequence number.

no deny sequence *num*

Use the following syntax to delete a TCP rule without specifying the sequence number:

no deny [**enable-accounting**] [**vlan** *vlan-id*] **tcp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**established**] [**syn**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Use the following syntax to delete an ICMP rule without specifying the sequence number:

no deny [**enable-accounting**] [**vlan** *vlan-id*] **icmp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*icmp-parameters*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Use the following syntax to delete an SCTP or UDP rule without specifying the sequence number:

no deny [**enable-accounting**] [**vlan** *vlan-id*] { **sctp** | **udp** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Use the following syntax to delete an AHP, ESP, or UDP rule without specifying the sequence number:

no deny [**enable-accounting**] [**vlan** *vlan-id*] { **ahp** | **esp** | **ipv6** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Parameters

enable-accounting

(Not supported on Brocade MLX Series or Brocade NetIron XMR Series devices.) Enable accounting for the rule.

vlan *vlan-id*

(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.) Specify a VLAN.

protocol

Specifies the type of IPv6 packet you are filtering. You can either specify a protocol number (from 0 through 255) or one of the following protocol names:

- AHP—Authentication Header
- ESP—Encapsulating Security Payload
- ICMP—Internet Control Message Protocol
- IPv6—Internet Protocol, version 6
- SCTP—Stream Control Transmission Protocol
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol

ipv6-source-prefix **/** *prefix-length*

Specifies a source prefix and prefix length that a packet must match for the specified action (deny or permit) to occur. You must specify the *ipv6-source-prefix* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. Specify the *prefix-length* parameter as a decimal value, preceded by a slash mark (/).

any

When specified instead of the *ipv6-source-prefix*/*prefix-length* or *ipv6-destination-prefix*/*prefix-length* parameters, matches any IPv6 prefix and is equivalent to the IPv6 prefix::/0.

host *source-ipv6_address num*

Enables you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

source-operators and *destination-operators*

If you specified **sctp**, **tcp**, or **udp** protocol, the following optional operators are available:

eq

The policy applies to the port name or number you enter after **eq**.

gt

The policy applies to 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 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 port numbers except the port number or port name you enter after **neq**.

range

The policy applies to all port numbers that are between the first 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.

ipv6-destination-prefix **/** *prefix-length*

Specifies a destination prefix and prefix length that a packet must match for the specified action (deny or permit) to occur. You must specify the *ipv6-destination-prefix* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. Specify the *prefix-length* parameter as a decimal value, preceded by a slash mark (/).

icmp-parameters

If you specify **icmp** as protocol, many parameters are available. For a current list, type a question mark (?) at the command prompt.

icmp-message-type

Specifies an ICMP message type. Values range from 0 through 255.

drop-precedence *dp-value*

Filters by the drop-precedence value that you specify. Values range from 0 through 3.

drop-precedence-force *dp-value*

If there are conflicting priority values for ingress packets, the default action is a priority merge. However, **drop-precedence-force** assigns the specified value to matching traffic. Values range from 0 through 3.

dscp *dscp-value*

The policy applies to packets that match the DSCP value. Values range from 0 through 63.

dscp-marking *dscp-value*

Assigns the value that you specify to the packet. Values range from 0 through 63.

priority-force *number*

Forces outgoing priority. Values range from 0 through 7.

priority-mapping *802.1p-value*

Filters by 802.1p priority.

established

(For TCP rules only) Filter packets that have the ACK (Acknowledgment) or RST (Reset) flag set. This policy applies only to established TCP sessions, not to new sessions.

syn

(For TCP rules only) Filter packets with the SYN (Synchronize) flag set.

fragments

(Not applicable for filtering based on source port, destination port, TCP protocol, or ICMP protocol) The policy applies to fragmented packets that contain a non-zero fragment offset.

routing

(Not applicable for filtering based on source port, destination port, TCP protocol, or ICMP protocol) The policy applies only to IPv6 source-routed packets.

match-payload-length

(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.) Match packets for configured IP payload length.

suppress-rpf-drop

(Not relevant for deny rules.) (Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.) Permit packets that fail the IPv6 RPF check.

log

(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices) Enables inbound logging for the rule. An additional requirement for deny logging is that the **ipv6 traffic-filter enable-deny-logging** command be in effect.

log-input

(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices) Enables inbound logging for the rule, with log entries including the incoming interface. An additional requirement for deny logging is that the **ipv6 traffic-filter enable-deny-logging** command be in effect.

mirror

Mirrors packets matching the rule.

copy-sflow

(Not relevant for deny rules.) Sends matching inbound packets to the sFlow collector.

sequence *num*

Enables you to assign a sequence number to the rule. If you do not specify **sequence** *num*, the rule is added at the end of the list.

Modes

ACL configuration mode

Usage Guidelines

If you need to specify **sequence** *num*, you can do so in one of the following syntax positions:

- As the first element
- At any point following the destination specification.

Examples

The following example defines rules that filter by the SCMP protocol.

```
device# configure terminal
device(config)# ipv6 access-list sctp_filter
device(config-ipv6-access-list sctp_filter)# permit sctp 201:1::1:1/64 eq 28 any range 10 100
device(config-ipv6-access-list sctp_filter)# permit sctp 201:1::1:1/64 lt 28 301:1::1:1/64 gt 100
device(config-ipv6-access-list sctp_filter)# deny sctp any lt 28 any gt 100
```

History

Release version	Command history
6.0.00a	This command was modified to support the SCTP protocol.

diagnostics (MRP)

Enables diagnostics on a metro ring.

Syntax

diagnostics

no diagnostics

Command Default

Diagnostics are disabled by default.

Modes

Metro ring configuration mode

Usage Guidelines

This command is valid only on the master node.

When you enable Metro Ring Protocol (MRP) diagnostics, the software tracks Ring Health Packets (RHPs) according to their sequence numbers and calculates how long it takes an RHP to travel one time through the entire ring. The calculated results have a granularity of 1 microsecond. When you display the diagnostics, the output shows the average round-trip time for the RHPs sent since you enabled diagnostics.

The **no** form of the command disables the diagnostics for the ring.

Examples

The following example enables the diagnostics for metro ring 1.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)# diagnostics
```

disable authenticate md5

Disables the MD5 authentication scheme for Network Time Protocol (NTP).

Syntax

disable authenticate md5

no disable authenticate md5

Command Default

If JITC is enabled, the MD5 authentication scheme is disabled. In the standard mode, the MD5 authentication scheme is enabled.

Modes

NTP configuration mode.

Usage Guidelines

In the standard mode, both SHA1 and MD5 authentication schemes are supported. If JITC is enabled using the **jitc enable** command, the MD5 authentication for Network Time Protocol (NTP) is disabled by default and the **disable authenticate md5** command can be seen in the running configuration. In the JITC mode, only the SHA1 authentication option is available. The SHA1 authentication scheme must be enabled manually by configuring the authentication key for NTP using the **authentication-key** command and an example of configuring this command is shown below.

The **no** form of the command enables the MD5 authentication scheme.

Examples

The following example disables the MD5 authentication scheme.

```
device# configure terminal
device(config)# ntp
device(config-ntp)# disable authenticate md5
```

The following example enables SHA1 authentication for NTP.

```
device# configure terminal
device(config)# ntp
device(config-ntp)# authentication-key key-id 20 sha1 keystring
```

History

Release version	Command history
5.8.00	This command was introduced.

disable-acl-for-6to4

Disables IPv6 access control list (ACL) processing for IPv6-over-IPv4 internal traffic.

Syntax

disable-acl-for-6to4

no disable-acl-for-6to4

Command Default

ACL processing is enabled for IPv6-over-IPv4 traffic.

Modes

ACL policy configuration mode

Usage Guidelines

This command only affects a tunnel-terminating node.

The command does not affect the following types of ACLs:

- Layer 2 (MAC) ACLs
- IPv4 ACLs
- User-defined ACLs (UDA ACLs)

Disabling ACL processing also disables support for the following features for internal traffic coming over the tunnel:

- All features employing IPv6 ACLs
- BFD over MPLS
- Multicast
- PBR
- OpenFlow

The **no** form of this command re-enables ACL processing.

Examples

The following example disables IPv4 and IPv6 ACL processing on a tunnel-terminating node.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# disable-acl-for-6to4
```

The following example re-enables ACL processing.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# no disable-acl-for-6to4
```

History

Release version	Command history
6.0.0	This command was introduced.

disable-acl-for-gre

Disables IPv4 and IPv6 access control list (ACL) processing for Generic Routing Encapsulation (GRE)-tunneled internal traffic.

Syntax

disable-acl-for-gre

no disable-acl-for-gre

Command Default

ACL processing is enabled for GRE-tunneled traffic.

Modes

ACL policy configuration mode

Usage Guidelines

This command only affects a tunnel-terminating node.

The command does not affect the following types of ACLs:

- Layer 2 (MAC) ACLs
- User-defined ACLs (UDA ACLs)

This command applies to both named and numbered ACLs.

Disabling ACL processing also disables support for the following features for internal traffic coming over the tunnel:

- All features employing IPv4/IPv6 ACLs
- BFD over MPLS
- Multicast
- PBR
- OpenFlow

The **no** form of this command re-enables ACL processing.

Examples

The following example disables IPv4 and IPv6 ACL processing on a tunnel-terminating node.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# disable-acl-for-gre
```

The following example re-enables ACL processing.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# no disable-acl-for-gre
```

History

Release version	Command history
6.0.0	This command was introduced.

disable-incremental-spf-opt

Disables incremental full SPF optimizations for Intermediate System-to-Intermediate System (IS-IS).

Syntax

disable-incremental-spf-opt

no disable-incremental-spf-opt

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

If you disable the partial SPF optimizations using the **disable-partial-spf-opt** command, IS-IS automatically disables the incremental SPF optimizations and always runs full SPF. However, if you disable incremental SPF optimizations using this command, IS-IS does not disable partial optimizations.

The **no** form of the command restores incremental SPF optimizations for IS-IS.

Examples

The following example disables incremental SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-incremental-spf-opt
```

The following example restores incremental SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no disable-incremental-spf-opt
```

disable-inc-stct-spf-opt

Disables incremental shortcut LSP SPF optimization.

Syntax

disable-inc-stct-spf-opt

disable-inc-stct-spf-opt

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command restores incremental shortcut LSP SPF optimization.

Examples

The following example disables incremental shortcut LSP SPF optimization.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-inc-stct-spf-opt
```

disable-partial-spf-opt

Disables partial SPF optimizations for Intermediate System-to-Intermediate System (IS-IS).

Syntax

disable-partial-spf-opt

no disable-partial-spf-opt

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

If you disable the partial SPF optimizations using this command, IS-IS automatically disables the incremental SPF optimizations and always runs full SPF. However, if you disable incremental SPF optimizations using the **disable-incremental-spf-opt** command, IS-IS does not disable partial optimizations.

The **no** form of the command restores partial SPF optimizations for IS-IS.

Examples

The following example disables partial SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-partial-spf-opt
```

The following example restores partial SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no disable-partial-spf-opt
```

distance (BGP)

Changes the default administrative distances for eBGP, iBGP, and local BGP.

Syntax

distance *external-distance internal-distance local-distance*

no distance

Command Default

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

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

To select one route over another according to the source of the route information, the device can use the administrative distances assigned to the sources. The administrative distance is a protocol-independent metric that IP devices use to compare routes from different sources. Lower administrative distances are preferred over higher ones.

Examples

This example configures the device to change the administrative distance.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# distance 100 150 200
```

distance (IS-IS)

Configures an administrative distance value for Intermediate System-to-Intermediate System (IS-IS) routes.

Syntax

distance *number*

no distance *number*

Command Default

The default is 115.

Parameters

value

Specifies the administrative distance. Valid values range from 1 through 255. The default is 115.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

Routes with a distance value of 255 are not installed in the routing table.

The **no** form of the command resets the distance value to the default value of 115.

Examples

The following example sets an administrative distance of 40 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-isis-router-ipv4u)# distance 40
```

The following example sets an administrative distance of 60 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-isis-router-ipv6u)# distance 60
```

distance (OSPF)

Configures an administrative distance value for OSPFv2 and OSPFv3 routes.

Syntax

distance { **external** | **inter-area** | **intra-area** } *distance*

no distance

Command Default

The administrative distance value for OSPFv2 and OSPFv3 routes is 110.

Parameters

external
Sets the distance for routes learned by redistribution from other routing domains.

inter-area
Sets the distance for all routes from one area to another area.

intra-area
Sets the distance for all routes within an area.

distance
Administrative distance value assigned to OSPF routes. Valid values range from 1 through 255. The default is 110.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

You can configure a unique administrative distance for each type of OSPF route.

The distances you specify influence the choice of routes when the device has multiple routes from different protocols for the same network. The device prefers the route with the lower administrative distance. However, an OSPFv2 or OSPFv3 intra-area route is always preferred over an OSPFv2 or OSPFv3 inter-area route, even if the intra-area route's distance is greater than the inter-area route's distance.

The **no** form of the commands reverts to the default setting.

Examples

The following example sets the distance value for all external routes to 125.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# distance external 125
```

The following example sets the distance value for intra-area routes to 80.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# 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-ospf6-router)# distance inter-area 90
```

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** [**ethernet** *slot/port* | **loopback** *number* | **pos** *slot/port* | **tunnel** *number* | **ve** *virtual port number*]

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.

ethernet
Specifies an Ethernet interface.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

loopback *number*
Specifies a loopback interface and port number.

pos
Specifies a POS port.

slot
Specifies a valid slot number.

port
Specifies a valid port number.

tunnel *number*
Specifies a tunnel.

ve *virtual port number*
Specifies a virtual Ethernet (VE) interface.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **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-ospf6-router)# distribute-list prefix-list filterOspfRoutes in
```

distribute-list route-map

Creates a route-map distribution list.

Syntax

distribute-list route-map *map* **in**

no distribute-list route-map

Parameters

map

Specifies a route map.

in

Creates a distribution list for an inbound route map.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The distribution list can filter Link State Advertisements (LSAs) received from other OSPF devices before adding the corresponding routes to the routing table.

The **no** form of the command removes the distribution list.

Examples

The following example creates a distribution list using a route map named filter1 that has already been configured.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# distribute-list route-map filter1 in
```

display-pkt-bit-rate

Displays the Packet and Bit rate statistics for the policy based routing.

Syntax

display-pkt-bit-rate

no display-pkt-bit-rate

Command Default

None.

Modes

ACL policy sub-configuration mode (config-acl-policy).

Usage Guidelines

When deploying this command, a new display format displays the PBR statistics. Otherwise, the old or existing CLI display format is used (only packet rate statistics are displayed).

This configuration stores in the configuration file.

Examples

The following example shows how the new format can be enabled using the CLI command:

```
device(config-acl-policy) #display-pkt-bit-rate
```

Release version	Command history
5.8.00	This command is introduced.

dot1ag-transparent

Forwards non-CCM packets without altering the packet prioritization at the ingress.

Syntax

dot1ag-transparent

no dot1ag-transparent

Command Default

The command is not enabled by default.

Modes

Global configuration mode.

Usage Guidelines

When IEE 802.1ag CFM is not configured for the device, the priority of non-CCM packets can change due to Protocol Packet Prioritization (PPP) at the ingress. Since the node needs to forward the packet without altering the packet priority, Brocade recommends using this command when forwarding non-CCM packets.

The**no** form of the command reverts the command behavior back to default; non-CCM packets are forwarded with altered packet prioritization.

The command is saved upon reload.

NOTE
The command is supported on Brocade NetIron XMR Seriesand Brocade NetIron MLX Series devices.

Examples

The following example forwards the non-CCM packet without altering the packet priority.

```
device(config)# dot1ag-transparent
```

History

Release version	Command history
5.7.00	This command was introduced.

dot1x-key

Configures switch port to dynamically obtain MKA keys from RADIUS server.

Syntax

dot1x-key

no dot1x-key

Command Default

By default, this command is disabled.

Modes

Macsec ethernet and group configuration mode

Usage Guidelines

The **dot1x-key** command is effective only if the interface is dot1x-enabled using the **dot1x-enable** command.

NOTE
An MKA configuration group should be attached to the interface before applying dot1x-key configuration on the interface.

The **no** form of the command disables dot1x-key configuration from the port.

Examples

The following example configures dot1x-key on Ethernet interface 1/1.

```
device# configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# enable-mka ethernet 1/1
device(config-dot1x-mka-eth-1/1)# dot1x-key
```

History

Release version	Command history
5.8.00	This command was introduced.

dot1x-mka-enable

Enables MACsec Key Agreement (MKA) capabilities on a Brocade device and enters dot1x-mka configuration mode.

Syntax

dot1x-mka-enable

no dot1x-mka-enable

Command Default

By default, MACsec MKA capabilities are not enabled.

Modes

Global configuration mode

Usage Guidelines

When the **dot1-mka-enable** command is disabled, all the configurations under that mode are deleted. If MKA is disabled, all the ports go into a down state. To bring the ports back to online, you must manually enable each port.

The **no** form of this command disables the MKA and MACsec functionality on all ports.

Examples

The following example enables MACsec MKA capabilities is enabled on the device.

```
device# configure terminal
device(config)# dot1x-mka-enable
Brocade(config-dot1x-mka)#
```

History

Release version	Command history
5.8.00	This command was introduced.

eckeypair

Specifies which Elliptic Curve key pair to use during enrollment.

Syntax

eckeypair { **key-label** *label* | **encryption-key-size** *encryption key-size* | **key-size** *key-size* }

Parameters

key-label *label*

Specifies the name of the key pair generated during enrollment. The name is specified if it is not already existing or if the **auto-enroll regenerate** command is configured.

encryption-key-size *encryption key-size*

Specifies the size of the second key that is generated to request separate encryption, signature keys, and certificates.

key-size*key-size*

Specifies the size of the desired EC key pair. If the key size is not specified, the existing key size is used. The supported values are 256 and 384.

Modes

PKI trustpoint configuration mode

Usage Guidelines

The key pair is obtained by importing from the key file that has a specific label.

Examples

The following example specifies which EC key pair to use during enrollment.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# eckeypair key-label brocade
```

The following example specifies the encryption key size.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# eckeypair encryption-key-size 100
```

The following example specifies the desired EC key size of 256.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# eckeypair key-size 256
```

History

Release version	Command history
05.8.00	This command was introduced.
05.8.00b	This command was modified to add the **encryption-key-size** and **key-size** keywords.

egress-truncate

Enables the truncation of egress packets for a port.

Syntax

egress-truncate

no egress-truncate

Command Default

The command is not enabled by default. The specified size of the truncated packet is set globally using the **egress-truncate-size** command.

Modes

This command is used at the config level.

Usage Guidelines

The **no** form of the command disables truncation on the specific port. The **egress-truncate** command is supported for LAG ports.

Examples

The **egress-truncate-size** command enables truncation on all ports that are members of the LAG. The following example shows both LAG configuration and enabling truncate

```
device(config)# lag  lag1 static id 1
device(config-lag-lag1)# ports Ethernet 1/1 to 1/4
device(condfig-lag-lag1)# primary Ethernet 1/1
device(config-lag-lag1)# deploy

device(config-if-1/1)# egress-truncate
```

History

Release version	Command history
5.9.00	This command was introduced.

egress-truncate-size

Sets the size of the truncated egress packets globally.

Syntax

egress-truncate-size *value* **slot** [*all* |*slot_no* [<device_id>]]

no egress-truncate-size

Command Default

The command disabled by default. When enabled, the default setting is 64 bytes.

Parameters

value
The packet size in bytes after being truncated.

slot_no
An optional value for the slot number.

device_id
An optional value for the device ID.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of this command disables truncating globally. Use the **egress-truncate** command to enable truncation. The **egress-truncate-size** command is supported globally for LAG ports.

Examples

The command must be enabled on a port or LAG using the **egress-truncate** command. The following example sets the size of the truncated egress packets to 200 bytes on all slots.

```
Brocade(config)#egress-truncate-size 200 slot all
```

History

Release version	Command history
5.9.00	This command was introduced.

email

Configures the email ID for the Public Key Infrastructure (PKI) entity.

Syntax

email *string* **no email** *string*

Parameters

string

Specifies the email ID for the PKI entity.

Modes

PKI entity configuration mode.

Usage Guidelines

The **no** form of the command removes the configured email ID.

Examples

The following example configures the email ID (user@brocade.com) for the PKI entity.

```
device(config)# pki entity test
device(config-pki-entity-test)# email user@brocade.com
```

History

Release version	Command history
5.8.00	This command was introduced.

enable-mka

Enables MACsec Key Agreement (MKA) on a specified interface and changes the mode to dot1x-mka-interface mode to enable related parameters to be configured.

Syntax

enable-mka ethernet *slot*/*port* [**to** *slot*/*port*]

no enable-mka ethernet *slot*/*port* [**to** *slot*/*port*]

Command Default

MKA is not enabled on an interface.

Parameters

ethernet *slot port*

Specifies an Ethernet interface and the slot on the device, and the port on that slot.

Modes

dot1x-mka-interface mode

Usage Guidelines

For a MACsec channel to be created between two ports, both ports and devices designated must have MACsec enabled and configured.

The **no** form of the command removes MACsec from the port.

NOTE

Primary port configuration will not be applied to all secondary ports in a LAG. LAG member ports should have individual configurations to enable MACsec.

Examples

The following example enables MACsec on Ethernet interface 1/1.

```
device(config-dot1x-mka)# enable-mka ethernet 1/1
device(config-dot1x-mka-eth-1/1)#
```

The following example configures MKA on multiple ports and enters the multiple interface configuration mode.

```
device(config-dot1x-mka)# enable-mka ethernet 1/1 to 1/10
device(config-dot1x-mka-mif-eth-1/1-1/10)#
```

History

Release version	Command history
5.8.00	This command was introduced.

enable (VSRP)

Enables the VSRP VRID for a port-based VLAN.

Syntax

enable

disable

Command Default

The VSRP VRID is disabled by default.

Modes

VSRP VRID configuration mode

Usage Guidelines

The device must be set as a backup. Because VSRP does not have an owner, all VSRP devices are backups. The active device for a VRID is elected based on the VRID priority.

The **disable** command deactivates VSRP.

Examples

The following example shows how to enable the VSRP VRID on a VLAN.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# backup
device(config-vlan-200-vrid-1)# enable
```

enable-qos-statistics

Enables the collection of egress counter statistics on Brocade NetIron CER and CES series devices and enables the collection of statistics for ingress and egress packet priorities on Brocade NetIron XMR and MLX series devices.

For Brocade NetIron XMR and MLX series devices the command has no parameters.

[no] enable-qos-statistics

Brocade NetIron CER and CES series devices only.

[no] enable-qos-statistics interface *slot/port* **traffic-type** { **l2-l3** | **vpls-vll-of** } [**vlan** *vlan-id*] [**queue** *queue-num*] [**dp** *dp-value*]

Brocade NetIron CER and CES series devices.

no enable-qos-statistics interface *slot/port* [**traffic-type** { **l2-l3** | **vpls-vll-of** } [**vlan** *vlan-id*] [**queue** *queue-num*] [**dp** *dp-value*]]

These parameters are for Brocade NetIron CER and CES series devices only.

interface *slot/port*
Enables counting of egress traffic on an interface identified by the slot on the device, and the port on that slot.

traffic-type
This keyword enables the counting of egress traffic that matches either physical Layer 2 and Layer 3 traffic or virtual VPLS/ VLL/ Openflow traffic.

l2-l3
This keyword specifies physical port traffic - Regular Layer 2 and Layer 3 egress traffic is counted.

vpls-vll-of
This keyword specifies that virtual port traffic - Virtual Private LAN Service (VPLS) or Virtual Leased Line (VLL) egress traffic is counted.

vlan *vlan-id*
This option specifies that traffic that matches the VLAN ID is counted. The *vlan-id* ranges from 1 to 4090.

queus *que-num*
This option specifies that traffic that matches the queue number is counted. The *que-num* or traffic class ranges from 0 to 7.

dp *dp-value*
This option specifies that traffic that matches the drop precedence value is counted. The *dp-value* can be 0 to 3.

There are no command parameters for the Brocade NetIron XMR and MLX series devices.

The counters are disabled by default.

Global configuration mode.

For Brocade NetIron CER and CES series devices, the **no** form of the command can be used to disable egress counters at the interface level.

For Brocade NetIron CER and CES series devices, only one egress statistics counter is supported per forwarding hardware.

For Brocade NetIron XMR and MLX series devices, the command has no parameters.

On Brocade NetIron CER and CES series devices, the following example enables all of he the egress counters for regular Layer 2 and Layer 3 traffic on interface 2/2.

```
device(config)# enable-qos-statistics interface 2/2 traffic-type l2-l3
```

On Brocade NetIron CER and CES series devices, the following example enables egress counters for regular Layer 2 and Layer 3 traffic on VLAN 200, queue 7, with a drop precedence value of 2.

```
device(config)# enable-qos-statistics interface 2/1 traffic-type l2-l3 vlan 200 queue 7 dp 2
```

On Brocade NetIron CER and CES series devices, the following example disables egress counters at the interface level.

```
device(config)# no enable-qos-statistics interface 2/1
```

On Brocade NetIron CER and CES series devices, the following example disables egress counters for regular Layer 2 and Layer 3 traffic on VLAN 200, queue 7, with a drop precedence value of 2.

```
device(config)# no enable-qos-statistics interface 2/1 traffic-type l2-l3 vlan 200 queue
7 dp 2
```

On Brocade NetIron XMR and MLX series devices, the following command enables the collection of statistics for ingress and egress packet priorities.

```
device(config)# enable-qos-statistics
device(config)#
```

On Brocade NetIron XMR and MLX series devices, the following command disables the collection of statistics for ingress and egress packet priorities.

```
device(config)# no enable-qos-statistics
device(config)#
```

Release version	Command history
5.9.00a	This command was modified to enable the collection of egress counter statistics on Brocade NetIron CER and CES series devices.
5.5.00	This command was introduced for Brocade NetIron XMR and MLX series devices.

encapsulation-mode

Specifies the encapsulation mode for an IPsec proposal.

Syntax

encapsulation-mode *encapsulation-mode*

Command Default

The default encapsulation mode is tunnel mode.

Parameters

encapsulation-mode

Specifies the encapsulation mode. Only tunnel mode is currently supported.

Modes

IPsec proposal configuration mode

Usage Guidelines

Because tunnel mode is configured by default and is the only mode that is currently supported, you do not need to configure the encapsulation mode for an IPsec proposal.

Examples

The following example shows how to configure tunnel mode as the encapsulation mode for an IPsec proposal named ipsec_proposal.

```
device(config)# ipsec proposal ipsec_proposal
device(config-ipsec-proposal-ipsec_proposal)# encapsulation-mode tunnel
```

History

Release version	Command history
5.8.00	This command was introduced.

encryption

Configures an encryption algorithm for an Internet Key Exchange version 2 (IKEv2) proposal.

Syntax

encryption { **aes-cbc-128** | **aes-cbc-256** }

no encryption { **aes-cbc-128** | **aes-cbc-256** }

Command Default

The default encryption algorithm is AES-CBC-256.

Parameters

aes-cbc-128

Specifies the 128-bit advanced encryption standard algorithm in cipher block chaining mode.

aes-cbc-256

Specifies the 256-bit advanced encryption standard algorithm in cipher block chaining mode.

Modes

IKEv2 proposal configuration mode

Usage Guidelines

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

Examples

The following example shows how to configure the AES-CBC-128 encryption algorithm for an IKEv2 proposal named ikev2_proposal.

```
device(config)# ikev2 proposal ikev2_proposal
device(config-ikev2-proposal-ikev2_proposal)# encryption aes-cbc-128
```

History

Release version	Command history
5.8.00	This command was introduced.

end-of-lib

Enable the end-of-lib configuration mode.

Syntax

end-of-lib

no end-of-lib

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of this command to remove this mode and attribute under it.

The end-of-lib mode contains all the attributes of the end of lib capability and notification. Also, when you enable the end-of-lib mode, you can determine whether the two RFCs 5561 and 5919 are enabled by the LSR.

Examples

The following example enables the end-of-lib configuration mode.

```
device(conf)# router mpls
device(conf-mpls)# ldp
device(conf-mpls-ldp)# end-of-lib
device(conf-mpls-ldp-eol)#
```

enforce-first-as

Enforces the use of the first autonomous system (AS) path for external BGP (EBGP) routes.

Syntax

enforce-first-as

no enforce-first-as

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

This command causes the router to discard updates received from EBGP peers that do not list their AS number as the first AS path segment in the AS_PATH attribute of the incoming route.

Examples

This example configures the device to enforce the use of the first AS path.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# enforce-first-as
```

enrollment

Configures the enrollment information such as retry count, retry period, or profile for the polling interval for the certificate authority (CA).

Syntax

enrollment { **retry-count** *count* | **retry-period** *period* | **profile** *profile name* }

no enrollment { **retry-count** *count* | **retry-period** *period* | **profile** *profile name* }

Parameters

retry-count
Specifies the retry count value to get the CA.

count
The retry count value in numbers. Valid numbers range from 1 through 100. The default is 10.

retry-period
Specifies the time period to keep trying to get the CA.

period
The time period value in minutes. Valid numbers range from 1 through 60 minutes. The default is 1 minute.

profile
Specifies the profile name to get the CA.

profile name
The profile name specified to get the CA.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The **no** form of the command disables the device from configuring enrollment options.

When the device configures the **enrollment** command for a second time to request the CA, the retry period between requests increases exponentially, with an additional 1 minute interval added at every increment.

Examples

The following example specifies the retry count value as 11.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# enrollment retry-count 11
```

The following example specifies the retry period of 2 minutes to get the CA.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# enrollment retry-period 2
```

The following example specifies the profile name as "Jane".

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# enrollment Jane
```

History

Release version	Command history
5.9.00	This command was introduced.

enrollment terminal

Enables the generation of a Public Key Infrastructure (PKI) certificate signing request (CSR) on the device terminal for offline enrollment. This command also enables manual authentication of a trustpoint and the loading of certificates from the device terminal.

Syntax

enrollment terminal

no enrollment terminal

Command Default

The enrollment terminal feature is disabled.

Modes

PKI trustpoint configuration mode

Usage Guidelines

The enrollment terminal feature is used for a trustpoint that is offline.

When **enrollment terminal** is enabled, issue the **pki enroll** command to display a CSR on the device terminal (in Public-Key Cryptographic Standard #10 (PKCS #10) format) and save it to flash memory in privacy-enchanced mail (PEM) format. The name of the CSR file saved to flash memory is pki_certreg_*trustpoint_name*.

The **no** form of the command disables terminal enrollment.

Examples

The following example shows how to enable enrollment terminal on a trustpoint named example_tp.

```
device(config)# pki trustpoint example_tp
device(config-pki-trustpoint-example_tp)# enrollment terminal
```

History

Release version	Command history
6.0.00a	This command was introduced.

esn-enable

Configures the Extended Sequence Number (ESN) for IPsec.

Syntax

esn-enable

no esn-enable

Command Default

Modes

IPsec proposal configuration mode.

Usage Guidelines

ipsec esn-enable

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

Examples

The following example configures the ESN for IPsec.

```
device(config)# ipsec proposal brocade
device(config-ipsec-proposal-brocade)# esn-enable
```

History

Release version	Command history
5.8.00	This command was introduced.

exclude-interface

The user can create a bypass LSP by using the bypass-lsp command. The bypass LSP is the specification of excluded interfaces, which can be embodied as individual interfaces, ranges of interfaces, groups, or LAGs. Using this command the user can choose the interface to avoid as well as protect.

Syntax

exclude-interface { **ethernet** *slot/port* [**ethernet** *slot/port* | **to** *slot/port*] | **pos** *slot/port* [**pos** *slot/port* | **to** *slot/port*] | **ve** *inteface_id* }

no exclude-interface { **ethernet** *slot/port* [**ethernet** *slot/port* | **to** *slot/port*] | **pos** *slot/port* [**pos** *slot/port* | **to** *slot/port*] | **ve** *inteface_id* }

Command Default

By default, an interface is not protected.

Parameters

ethernet *slot/port*

Specifies Ethernet port.

to *slot/port*

Specifies the receiving port.

pos *slot/port*

Specifies the selected individual POS interface port.

to *slot/port*

Specifies the receiving port.

ve *interface_id*

Specifies the selected Virtual Ethernet (VE) interface.

Modes

MPLS bypass LSP sub-configuration mode

Usage Guidelines

This is used for facility backup FRR. In the context of bypass LSP, the user can configure an MPLS interface as an exclude (protected) interface against resource failures using a bypass LSP. The user can specify a VE interface as exclude-interface. When a protected LSP egress interface is a VE interface, then any fault on a VE interface could trigger FastReroute. The following example configures protection for MPLS interface ve 100 using facility backup FRR.

The **no** form of the command removes the bypass LSP.

Examples

The following example displays the command.

```
device# configure terminal
device(config)# router-mpls
device(config-mpls)# bypass-lsp 123
device(config-mpls-bypasslsp-123)# exclude-interface ethernet 1/1 ethernet 1/3
device(config-mpls-bypasslsp-123)# exclude-interface ethernet 1/1 ethernet 1/3 to 1/4
```

export-vrf-leaked-routes

Redistributes routes imported from one VRF to another into VRF-BGP and advertises the route to the Layer 3 VPN network

Syntax

export-vrf-leaked-routes

no export-vrf-leaked-routes

Command Default

Enabled. Routes are not automatically blocked.

Modes

Address family IPv4 VPN unicast configuration mode

Address family IPv6 VPN unicast configuration mode

Usage Guidelines

The **no** form of the command blocks inter-VRF leaked routes.

The default behavior is backward compatible. A BGP option has been added to disable backward compatibility.

Starting in 5.8.00d and 5.9.00a, this command also disables inter-VRF-leaking of BGP routes with LSP next-hop.

Examples

This example blocks inter-VRF leaked routes from being advertised out to a Layer 3 VPN network. for the IPv4 VPN unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family vpnv4 unicast
device(config-bgp-vpn4u)# no export-vrf-leaked-routes
```

This example blocks inter-VRF leaked routes from being advertised out to a Layer 3 VPN network. for the IPv6 VPN unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family vpnv6 unicast
device(config-bgp-vpnv6)# no export-vrf-leaked-routes
```

History

Release version	Command history
NI 5.6.00e	This command was introduced.
5.8.00d and 5.9.00a	This command was modified so that inter-VRF-leaking of BGP routes with LSP next-hop is disabled.

external-lsdb-limit (OSPFv2)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Command Default

14913080

Parameters

value

Maximum size of the external LSDB. Valid values range from 1 through 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-ospf-router)# external-lsdb-limit 20000
```

external-lsdb-limit (OSPFv3)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Command Default

250000

Parameters

value

Maximum size of the external LSDB. Valid values range from 1 through 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-ospf6-router)# external-lsdb-limit 15000
```

ext-stats-mode slot

Enables the extended statistics mode to display QinQ VLAN statistics.

Syntax

ext-stats-mode slot { *number* }

no ext-stats-mode slot { *number* }

Command Default

The extended statistics mode is not enabled.

Parameters

number

Specifies the interface module slot number for a 32-slot chassis (1-32), a 16-slot chassis (1-16), an 8-slot chassis (1-8), and a 4-slot chassis (1-4).

Modes

Global configuration mode

Usage Guidelines

Use this command to enable egress QinQ statistics when the extended counters are configured for a particular VPLS, VLL, or VLL-local instance. Extended statistics is enabled for ingress QinQ statistics by default. This CLI is added to support egress QinQ statistics. The QinQ statistics support is enabled only for QinQ VLANs configured under VPLS, VLL, and VLL-local.

This command configuration is supported on the Brocade MLX Series and Brocade NetIron XMR Series devices. On the BR-MLX-10Gx24 interface module, only the ingress QinQ statistics extended counters are supported. Gen1.1 modules are not supported.

When the command is enabled, the number of counters supported for egress port VLAN statistics per NP is reduced to 8191. There is no change to the number of counters for ingress. When the command is not enabled for QinQ statistics, the number of counters supported for ingress and egress does not change. The following table details the number of egress port VLAN counters supported on both ingress and egress counters, before and after enabling the **ext-stats-mode slot** command.

Switched and routed packets	Account based on internal priority of packet	Number of unique egress port-VLAN that have counters (pre-5.9)	Number of unique egress port-VLAN counters after enabling QinQ statistics mode
Switch and Route combined	No	32767 on ingress and 32767 on egress; each set having 8 counters.	32767 on ingress and 8191 on egress; each set having 1 counter.
Switch and Route combined	Yes	4095 on ingress and 4095 on egress; each set having 8 counters.	4095 on ingress and 4095 on egress; each set having 8 counters.

Switched and routed packets	Account based on internal priority of packet	Number of unique egress port-VLAN that have counters (pre-5.9)	Number of unique egress port-VLAN counters after enabling QinQ statistics mode
Switch or Route separately	No	16383 on ingress and 16383 on egress; each set having 2 counters.	16383 on ingress and 8191 on egress; each set having 2 counters.
Switch or Route separately	Yes	2047 on ingress and 2047 on egress; each set having 16 counters.	2047 on ingress and 2047 on egress; each set having 16 counters.

You must reload the interface module for the command to go into effect. A warning message of the required reload is displayed when the command is executed.

A syslog and warning message is generated if all 8191 egress statistics are utilized on a specific LP. A warning message similar to the following is displayed:

"Warning: Extended-Counter Egress Stats ID allocation failed for VPLS Eth 2/1 Vlan Id 200, Inner Vlan Id 500 "

There is a set number of counters supported per NP from hardware. If you receive this message, you can move the ports to the other NP. Each vport (port-VLAN combination) utilizes one statistics ID.

The **show mpls statistics vpls** and **clear mpls statistics vpls** commands are modified to include the parameter **inner-vlan** *vlan-id*. The parameter specifies the ID of the configured inner VLAN. If the **inner-vlan***vlan-id* parameter is not specified, the output displays vlan statistics only. To display specific tx/egress statistics, the **ext-stats-mode** command must be enabled for the LP module. If the command is not enabled for a specific slot, the QinQ statistics displays an NA value for ports of that slot.

The **no** form of the command disables the extended statistics mode to display QinQ VLAN statistics.

Examples

The following example enables the extended statistics mode to display QinQ VLAN statistics on interface module slot 4.

```
device(config)# ext-stats-mode slot ?
DECIMAL   LP slot (32-slot: 1-32, 16-slot: 1-16; 8-slot: 1-8; 4-slot: 1-4)
device(config)# ext-stats-mode slot 4
Please write memory. LP-2 reload is required for ext-stats-mode enable/disable to take effect.
```

Use the **show running-config** command to display the configuration for the **ext-stats-mode** command.

```
device(config)# show running-config | inc ext-stats-mode
ext-stats-mode slot 1
ext-stats-mode slot 2
ext-stats-mode slot 3
ext-stats-mode slot 4
```

History

Release version	Command history
5.9.00	This command was introduced.

extended-qos-mode set-force-tc-match-label-exp

This command enables queuing based on the EXP bit for VPLS or VLL traffic on the MPLS uplink,

Syntax

extended-qos-mode set-force-tc-match-label-exp

Modes

Global configuration mode

Usage Guidelines

Issue the **set-force-tc-match-label-exp** command after configuring all the VPLS instances and required peers on both ingress and egress peers, issue the command under **extended-qos-mode** command. This command will only succeed if there is sufficient space in the hardware table. You must write this command to memory and perform a system reload for this command to take effect.

Use the no form of the command to reset the default behavior.

Examples

```
device(config)#extended-qos-mode set-force-tc-match-label-exp
PPCR 0: Total TTI Size 32768, Used TTI 332
Space is enough to store TTI with extended action mode.
PPCR 2: Total TTI Size 32768, Used TTI 324
Space is enough to store TTI with extended action mode.
PPCR 3: Total TTI Size 32768, Used TTI 324
Space is enough to store TTI with extended action mode.
Reload required. Please write memory and then reload or power cycle the system.
PPCR 0: Total TTI Size 32768, Used TTI 332
Space is enough to store TTI with extended action mode with set-force-tc-match-labelexp.
```

History

Release version	Command history
6.1	This command is introduced in this release.

Commands F - J

fast-external-fallover

Resets the session if a link to an eBGP peer goes down.

Syntax

fast-external-fallover

no fast-external-fallover

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

Use this command to terminate and reset external BGP sessions of a directly adjacent peer if the link to the peer goes down, without waiting for the timer, set by the BGP **timers** command, to expire. This can improve BGP conversion time, but can also lead to instability in the BGP routing table as a result of a flapping interface.

Examples

This 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)# fast-external-fallover
```

fast-flood

Configures Intermediate System-to-Intermediate System (IS-IS) to flood Link State PDUs to other devices in the network before running SPF.

Syntax

fast-flood *lsp-count*

no fast-flood *sp-count*

Command Default

Four LSPs are flooded before running SPF.

Parameters

lsp-count

Specifies the number of LSPs that must be flooded before running SPF. Valid values range from 1 through 15. The default value is 4.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command resets the LSP count to the default value of 4.

Examples

The following example configures IS-IS to flood 10 LSPs before running SPF.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# fast-flood 10
```

fec-128-for-auto-discovered-peers

Configures the Brocade device to use FEC 128 to send the VC label binding for auto-discovered VPLS peers.

Syntax

fec-128-for-auto-discovered-peers

no fec-128-for-auto-discovered-peers

Command Default

By default, Brocade devices use FEC 129 to send the VC label binding for auto-discovered VPLS peers.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use this command in mixed environments where VPLS static configured peers and auto-discovered peers exist.

Save the configuration and reload the system for the **fec-128-for-auto-discovered-peers** command to take effect.

Use the **no** form of this command to reset the use of FEC 129.

Examples

The following example configures the use of FEC 128.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# fec-128-for-auto-discovered-peers
```

filter-fec

Configures LDP FEC filtering to filter label bindings on a MPLS router. You can filter inbound or outbound label bindings.

Syntax

filter-fec *prefix-list-name* **in** | **out**

no filter-fec *prefix-list-name* **in** | **out**

Command Default

By default, LDP distributes all FECs that are learned locally or from LDP neighbors to all other LDP neighbors.

Parameters

prefix-list-name
Specifies the prefix-list name.

in
Specifies an inbound-fec-filter configuration.

out
Specifies an outbound-fec-filter configuration.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the FEC filtering configuration.

LDP inbound-FEC filtering allows the control the amount of memory and CPU processing involved in installing and advertising label bindings not used for forwarding. It also serves as a tool to avoid DOS attack. For inbound FEC filter, consider the following:

- The FECs filtered by the LDP inbound-FEC filter do not install in the forwarding plane or advertise to the upstream neighbors. The FEC remains in the retained state.
- The LDP inbound-FEC filter are changed directly without deleting the one previously configured. The change automatically applies and triggers the filtering of inbound FECs.
- Changes to a referenced prefix-list automatically applies to LDP inbound-FEC filtering. This triggers filtering by way of the new configuration, filtering any existing FECs which violate the filter.
- To allow multiple route filter updates, the device waits for default 10 seconds before notifying the application of the filter change. The time for notification is configurable.
- When the LDP inbound-FEC filter is not configured, LDP does not filter any inbound FECs.
- By default, when the prefix-list referenced by the LDP inbound-FEC filter has no configuration, it is an implicit deny. All inbound FECs are filtered out and retained. The behavior is the same when the prefix list is deleted after setting it in the

inbound FEC filter configuration. This behavior is consistent with other protocols which use device filters and also with the use of the **advertise-fec** command for LDP route injection.

- Inbound FEC filtering is applicable only for Layer 3 FECs and not for VC FECs. Inbound FEC filtering is not applicable for Layer 2 VPNs.

LDP outbound FEC filtering gives you the ability to control which FECs can be advertised and to which LDP neighbors. It also reduces the number of labels distributed to neighbors and the number of messages exchanged with peers. Through this filtering, LDP scalability and convergence, security, and performance are improved.

Examples

The following example configures the LDP inbound-FEC filter.

```
device# configure terminal
device(config)# ip prefix-list list-abc permit 10.20.20.0/24
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# filter-fec list-abc in
```

The following example configures the LDP outbound-FEC filter.

```
device# configure terminal
device(config)# ip prefix-list list-out deny 10.40.40.0/24
device(config)# ip prefix-list list-out permit 0.0.0.0/0 ge 32
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# filter-fec list-out out
```

fingerprint

Configures the fingerprint for the Certificate Authority (CA).

Syntax

fingerprint *hex-data*

Parameters

hex-data

Specifies the hex data for the fingerprint in the xx:xx:xx:xx format.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

When the CA sends the certificate, it should match the fingerprint configured for the certificate to be accepted.

Examples

The following example configures the fingerprint for the CA.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# fingerprint 81:b7:d4:ab:05:53:fd:64:05:18:09:36:94:82:b3:56:bc:
93:74:c3
```

History

Release version	Command history
5.8.00	This command was introduced.

fqdn

Configures the fully qualified domain name (FQDN) for the PKI entity.

Syntax

fqdn *string*

Parameters

string

Specifies the FQDN for PKI entity.

Modes

PKI entity configuration mode.

Examples

The following example configures the FQDN for the PKI entity.

```
device(config)# pki entity brocade_entity
device(config-pki-entity-brocade_entity)# fqdn red
```

History

Release version	Command history
5.8.00	This command was introduced.

garp-ra-interval

Sets the interval between gratuitous ARP (GARP) router advertisements when Virtual Router Redundancy Protocol Extended (VRRP-E) scaling is configured.

Syntax

garp-ra-interval *interval*

no garp-ra-interval *interval*

Command Default

Gratuitous ARP router advertisements are sent every 30 seconds.

Parameters

interval

Sets the gratuitous ARP router advertisements interval timer, in seconds. Values range from 30 to 120 seconds. Default is 30 seconds.

Modes

Global configuration mode

Usage Guidelines

This command is used with the VRRP-E scaling feature where VRRP-E instances are grouped and hello messages between group members are stopped to reduce the CPU load and allow more VRRP-E instances to be configured. Gratuitous ARP messages are still sent by the group master on behalf of its members to advertise the virtual MAC address to devices on the network, but at a longer intervals.

The **no** form of this command resets the default value of 30 seconds between gratuitous ARP router advertisements.

Examples

The following example sets the gratuitous ARP router advertisement interval to 90 seconds.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# garp-ra-interval 90
```

History

Release version	Command history
5.8.00	This command was introduced.

gig-default

Enables auto-negotiation support for 1G ports.

Syntax

gig-default { **auto-gig** | **neg-off** | **auto-full** | **neg-full-auto** }

no gig-default { **auto-gig** | **neg-off** | **auto-full** | **neg-full-auto** }

Command Default

The default value is auto.

Parameters

auto-gig

The port tries to performs a negotiation with its peer port to exchange capability information. This is the default state.

neg-off

The port does not try to perform a negotiation with its peer port.

auto-full

The port tries to perform a negotiation with its peer port to exchange capability information. If it is unable to reach an agreed upon speed, the port goes into a fixed speed and keeps the link up.

neg-full-auto

The port is only for copper-SFP and to support 10/100/1000M tri-speed auto negotiation.

Modes

EXEC mode.

Usage Guidelines

Unless the ports at both ends of a Gigabit Ethernet link use the same mode (either auto-gig or neg-off), the ports cannot establish a link. An administrator must intervene to manually configure one or both sides of the link to enable the ports to establish the link.

The **no** form of the command disables *Remote Fault Notification (RFN)* after enabling.

Supports the following modules:

- 20x10GE
- 4x10GE-IPSEC

Examples

The following example displays how to change the negotiation mode for individual port.

```
device(config)# interface ethernet 4/1 to 4/4
device(config-mif-4/1-4/4)# gig-default neg-off
```

History

Release version	Command history
5.8.00a	This command was modified include the parameters **neg-off** and **auto**.

graceful-restart (LDP)

Enables the LDP graceful restart capability.

Syntax

graceful-restart [**helper-only**] [**max-neighbor-reconnect-time** *seconds*] [**max-neighbor-recovery-time** *seconds*] [**reconnect-time** *seconds*] [**recovery-time** *seconds*]

no graceful-restart [**helper-only**] [**max-neighbor-reconnect-time** *seconds*] [**max-neighbor-recovery-time** *seconds*] [**reconnect-time** *seconds*] [**recovery-time** *seconds*]

Command Default

Disabled.

Parameters

helper-only

Specifies that the LSR acts as a helper only. In helper mode, the configuration commands for reconnect-time and recovery-time is rejected with informational messages.

max-neighbor-reconnect-time *seconds*

Specifies the maximum time in seconds that this router must wait for a GR neighbor to restore the LDP session. Enter a integer from 60 to 300. The default setting is 120.

max-neighbor-recovery-time *seconds*

Specifies the maximum amount of time in seconds that this router waits for a GR neighbor to complete its GR recovery after the LDP session has been reestablished. Enter a integer from 60 to 3600. The default setting is 120.

reconnect-time *seconds*

Specifies the amount of time in seconds that a GR neighbor must wait for the LDP session to be reestablished. This value is advertised to the neighbor using the FT Reconnect Timeout field in the FT Session TLV. Enter a integer from 60 to 300. The default setting is 120.

recovery-time *seconds*

Specifies the amount of time in seconds that this router retains its MPLS forwarding state across restart. This value is advertised to the neighbor using the Recovery Time field in the FT Session TLV. Enter a integer from 60 to 3600. The default setting is 120.

Modes

MPLS LDP configuration mode

Usage Guidelines

When you enable LDP GR, the Brocade NetIron CES Series and Brocade NetIron CER Series routers are in helper mode only. The Brocade NetIron MLX Series and Brocade NetIron XMR Series routers can act either as a restarting router or a GR helper.

With LDP GR enabled, the router waits until it receives an LDP Initialization message from its neighbor to know whether it must delete its states or start the LDP GR recovery procedure. It is applicable to all LDP sessions regardless of the adjacency type exists between the neighbors.

The recovery time must be chosen accordingly taking into account the time it takes for RTM to recompute the routes and the number of Layer 3 FECs that need to be recovered as part of the LDP GR recovery. This is applicable to GR processing on ingress as well as transit LSRs.

NOTE
The reconnect-time and recovery-time commands are not available for Brocade NetIron CES Series and Brocade NetIron CER Series routers.

The **no** form of the commands removes the LDP GR helper mode and revert back to full LDP GR mode.

Examples

The following example sets the LDP GR timers and then enables LDP GR.

```
device(config-mpls-ldp)# graceful-restart reconnect-time 150
device(config-mpls-ldp)# graceful-restart recovery-time 240
device(config-mpls-ldp)# graceful-restart
```

graceful-restart (OSPFv2)

Enables the OSPF Graceful Restart (GR) capability.

Syntax

graceful-restart [**helper-disable** | **restart-time** *seconds*]

no graceful-restart

Command Default

Graceful restart and graceful restart helper capabilities are enabled.

Parameters

helper-disable

Disables the GR helper capability.

restart-time

Specifies the maximum restart wait time, in seconds, advertised to neighbors. The default value is 120 seconds. The configurable range of values is from 10 through 1800 seconds.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use **no graceful-restart helper-disable** to re-enable the GR helper capability.

The **no** form of the command disables the graceful restart capability.

Examples

The following example disables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# graceful-restart helper-disable
```

The following example re-enables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# no graceful-restart helper-disable
```

The following example re-enables the GR capability.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router ospf
device(config-router-ospf-vrf-default-vrf)# graceful-restart
```

The following example re-enables the GR capability and changes the maximum restart wait time from the default value to 240 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# graceful-restart restart-time 240
```

graceful-restart helper (OSPFv3)

Enables the OSPFv3 graceful restart (GR) helper capability.

Syntax

graceful-restart helper { **disable** | **strict-lsa-checking** }

no graceful-restart helper

Command Default

GR helper is enabled.

Parameters

disable

Disables the OSPFv3 GR helper capability.

strict-lsa-checking

Enables the OSPFv3 GR helper mode with strict link-state advertisement (LSA) checking.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command disables the GR helper capability on a device.

Examples

The following example enables GR helper and sets strict LSA checking.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router-ospf)# graceful-restart helper strict-lsa-checking
```

graceful-restart helper-disable (IS-IS)

Disables and enables Intermediate System-to-Intermediate System (IS-IS) graceful restart (GR) helper mode.

Syntax

graceful-restart helper-disable

no graceful-restart helper-disable

Command Default

The GR helper is enabled by default.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command re-enables the GR helper if it has been disabled.

Examples

The following example disables the IS-IS GR helper.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# graceful-restart helper-disable
```

The following example re-enables the IS-IS GR helper.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no graceful-restart helper-disable
```

group-master interface

Configures a Virtual Router Redundancy Protocol Extended (VRRP-E) device in interface configuration mode as the VRRP-E group master of a logical grouping of VRRP-E instances.

Syntax

group-master interface { **ethernet** *slot/port* | **ve** *vrid* } **vrid** *id*

no group-master interface { **ethernet** *slot/port* | **ve** *vrid* } **vrid** *id*

Command Default

No group master is configured.

Parameters

ethernet *slot/port*

Configures the VRRP-E group master for the specified port.

ve *vrid*

Configures the VRRP-E group master for the specified virtual Ethernet port.

vrid *id*

Assigns the VRID of the group master for the specified port.

Modes

Virtual router interface configuration mode

Usage Guidelines

This command is used as a grouping mechanism to allow the scaling of the number of VRRP extended (VRRP-E) instances up to 4000 instances. VRRP-E instances are configured into logical groups consistently across all the VRRP-E master and backup devices.

The **no** form of this command removes the grouping configuration.

Examples

The following examples configures virtual router 1 on interface ve 1 as the VRRP-E group master of the virtual router 2 on interface ve 2.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ve 2
device(conf-vif-2)# ip address 10.53.5.1/24
device(conf-vif-2)# ip vrrp vrid 2
device(conf-vif-2-vrid-2)# group-master interface ve 1 vrid 1
```

History

Release version	Command history
5.8.00	This command was introduced.

hello-interval (LDP)

Sets the interval between LDP Hello messages for LDP sessions for LDP interfaces. These messages maintain LDP sessions between the device and its LDP peers.

Syntax

hello-interval [**targeted**] *interval* [**hello-timeout** *seconds*]

no hello-interval [**targeted**] *interval* [**hello-timeout** *seconds*]

Command Default

For the global configuration, the default link interval is 5 seconds. The default targeted interval is 15 seconds.

The default timeout value is 45 seconds.

For an LDP interface configuration, the default value is the interval for the configured global LDP Hello messages.

Parameters

targeted

Specifies the LDP targeted Hello messages for the global configuration only. Without this option, the interval is for LDP linked Hello messages.

interval

Specifies the interval in seconds. Enter an integer from 1 through 32767.

hello-timeout *seconds*

Specifies the hold time value in seconds sent in the Hellos. Enter an integer from 1 to 65535. The default value is 45.

Modes

MPLS LDP configuration mode

MPLS interface LDP configuration mode

Usage Guidelines

Use this command to set the interval for LDP Link Hello messages that are multicast to all routers on the subnet.

Use the **targeted** option to set the interval for targeted Hello messages that are unicast to a specific address, such as a VLL peer. For targeted LDP sessions, the LDP Hello Interval can only be set globally.

For link LDP sessions, the LDP Hello Interval can be set globally which applies to all LDP interfaces or on an interface.

When you configure the LDP link interval for an interface, it overrides the global interval.

When a Hello Adjacency already exists, the adjacency remains up and any new configured interval takes effect upon the expiration of the current Hello Interval timer. Consequently, the next and subsequent Hello messages are sent at the new interval.

Use the **no** for this command to reset the default interval.

Examples

The following example sets the interval for targeted LDP sessions to 10 seconds globally.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-interval targeted 10
```

The following example sets the link Hello message interval for the interface to 30 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/2
device(config-mpls-if-e1000-1/2)# ldp-params
device(config-mpls-if-e1000-1/2-ldp-params)# hello-interval 30
```

hello-interval (VRRP)

Configures the interval at which master Virtual Router Redundancy Protocol (VRRP) routers advertise their existence to the backup VRRP routers.

Syntax

hello-interval [**msec**] *interval*

no hello-interval [**msec**] *interval*

Command Default

Hello messages from VRRP master routers are sent to backup routers every second.

Parameters

msec *interval*

Interval, in milliseconds, at which a master VRRP router advertises its existence to the backup VRRP routers. Valid values range from 100 through 84000. The default is 1000. VRRP-E does not support the hello message interval in milliseconds.

interval

Sets the interval, in seconds, for which a VRRP backup router waits for a hello message from the VRRP master router before determining that the master is offline. Valid values range from 1 through 84. The default value is 1.

Modes

VRID interface configuration mode

Usage Guidelines

A VRRP master router periodically sends hello messages to the backup routers. The backup routers use the hello messages as verification that the master is still online. If the backup routers stop receiving the hello messages for the period of time specified by the dead interval, the backup routers determine that the master router is dead. At that point, the backup router with the highest priority becomes the new master router.

By default, the dead interval is internally derived from the hello interval. It is equal to 3 times the hello interval plus the skew time, where the skew time is equal to (256 minus the priority) divided by 256. Generally, if you change the hello interval on the master VRRP router using the **hello-interval** command, you also should also change the dead interval on the VRRP backup routers using the **dead-interval** command.

The **hello-interval** command is configured only on master VRRP routers and is supported by VRRP and VRRP-E.

The **no** form resets the hello message interval to its default value of 1000 milliseconds (1 second).

NOTE
VRRP-E does not support the hello message interval in milliseconds.

Examples

The following example enables advertisements from the VRRP master router and sets the hello message interval to 10,000 milliseconds.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# hello-interval msec 10000
device(config-if-e1000-1/6-vrid-1)# activate
```

The following example enables advertisements from the VRRP-E master router and sets the hello message interval to 15 seconds.

```
device# configure terminal
device(config)# router vrrp-extended
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.3/24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 50 track-priority 10
device(config-if-e1000-1/5-vrid-2)# ip-address 10.53.5.1
device(config-if-e1000-1/5-vrid-2)# hello-interval 15
device(config-if-e1000-1/5-vrid-2)# activate
```

hello-interval (VSRP)

Configures the number of seconds between hello messages from the master to the backups for a given VRID.

Syntax

hello-interval *interval*

no hello-interval *interval*

Command Default

Hello messages from master are sent to backup in an interval 1 unit of 100 ms.

Parameters

interval

Sets the interval, in milliseconds, for which a backup waits for a hello message from the master before determining that the master is offline. Valid values range from 1 through 28 units of 100 milliseconds. The default value is 1 unit of 100 ms.

Modes

VSRP VRID configuration mode

Usage Guidelines

The Master periodically sends hello messages to the backup. The backup routers use the hello messages as verification that the master is still online. If the backup routers stop receiving the hello messages for the period of time specified by the dead interval, the backup routers determine that the master router is dead. At that point, the backup router with the highest priority becomes the new master router.

By default, the dead interval is internally derived from the hello interval. It is equal to 3 times the hello interval plus one-half second. Generally, if you change the hello interval on the master router using the **hello-interval** command, you also should also change the dead interval on the backup routers using the **dead-interval** command.

The **no** form resets the hello message interval to its default value 1 unit of 100 ms.

Examples

The following example sets the hello message interval to 15 seconds.

```
device# configure terminal
device(config)# vlan 400
device(config-vlan-400)# tagged ethernet 1/4 to 1/9
device(config-vlan-400)# vsrp vrid 4
device(config-vlan-400-vsrp-4)# hello-interval 15
```

hello-time

Sets the hello time value for metro ring packets.

Syntax

hello-time *ms*

no hello-time *ms*

Command Default

The hello time value is not preset.

Parameters

ms

The hello time value that is entered as multiples of 100 milliseconds. The valid values are 100 through 15000 entered as multiples of 100 ms. For example, a valid muliple of 100 ms can be 200, 700, 1300, 14000, and so on. Invalid value of 100 ms can be 221, 740, 1228, 1445, and so on. The default value is 100 ms.

Modes

MRP configuration mode

Usage Guidelines

The **no** form of the command resets the hello time that was defined for the hello ring packets.

Examples

The following example sets a value of 400 ms for the ring packets.

```
device(config)# vlan 1
device(config-vlan-1)# metro-ring 1
device(config-vlan-1-mrp-1)# hello-time 400
```

hello-timeout (LDP)

Sets how long the device waits for its LDP peers for LDP sessions to send a Hello message for LDP interfaces.

Syntax

hello-timeout [**targeted**] *seconds*

no hello-timeout [**targeted**] *seconds*

Command Default

For the global configuration, the default link interval is 15 seconds. The default targeted interval is 45 seconds.

For an LDP interface configuration, the default value is the hold time for the configured global LDP Hello messages.

Parameters

targeted

Specifies the LDP targeted Hello messages for the global configuration only. Without this option, the hold time is for LDP linked Hello messages.

seconds

Specifies the hold time in seconds. For a target session, enter an integer from 1 through 65335. For a link session, enter an integer from 2 through 65335.

Modes

MPLS LDP configuration mode

MPLS interface LDP configuration mode

Usage Guidelines

When the device does not receive a Hello message within this time, the LDP session with the peer can be terminated. The device includes the hold time in the Hello messages it sends out to its LDP peers.

The new time takes effect immediately and goes in the next Hello message sent. This hold time applies to only the hold time that the device sends to its peers. It does not affect the hold time the device uses to time out those peers. The latter is determined from the hold time that peers send to the device.

Use the **no** for this command to reset the default interval.

Examples

The following example sets the hold time for targeted LDP sessions to 20 seconds globally.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-timeout targeted 20
```

The following example sets the link Hello hold time for the interface to 30 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/2
device(config-mpls-if-e1000-1/2)# ldp-params
device(config-mpls-if-e1000-1/2-ldp-params)# hello-timeout 30
```

hello padding

Re-enables the padding of IS-IS hello PDUs globally.

Syntax

hello padding [**point-to-point**]

no hello padding [**point-to-point**]

Command Default

Enabled.

Parameters

point-to-point

Specifies Point-to-Point interfaces.

Modes

ISIS router configuration mode

Usage Guidelines

The **no** form of the command disables the padding of IS-IS hello PDUs. Generally, you do not need to disable padding unless a link is experiencing slow performance. If you enable or disable padding on an interface using the **isis hello padding** command, the interface setting overrides the global setting.

Examples

The following example globally disables padding of IS-IS hello PDUs.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no hello padding
```

The following example globally disables padding of IS-IS hello PDUs for Point-to-Point interfaces.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no hello padding point-to-point
```

The following example globally re-enables padding of IS-IS hello PDUs.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hello padding
```

The following example globally re-enables padding of IS-IS hello PDUs for Point-to-Point interfaces.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hello padding point-to-point
```

hold-down-interval

Configures the hold-down interval.

Syntax

hold-down-interval *number*

no hold-down-interval *number*

Command Default

The default hold-down time interval is 2 units of 100 ms (200 milliseconds).

Parameters

number

The time interval for the new master to hold the traffic. The time interval ranges from 2 through 84 units of 100 milliseconds.

Modes

VSRP VRID configuration mode

Usage Guidelines

The hold-down interval prevents the occurrence of Layer 2 loops during failover by delaying the new master from forwarding traffic long enough to ensure that the failed master is unavailable.

The **no** form of the command sets the time interval to the default value.

Examples

The following example shows how to change the hold-down interval.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vsrp-1)# hold-down-interval 4
```

hostname

Enables IS-IS name mapping capability on a device.

Syntax

hostname

no hostname

Command Default

Enabled.

Modes

ISIS router configuration mode

Usage Guidelines

The implementation of IS-IS supports RFC 2763, which describes a mechanism for mapping IS-IS system IDs to the hostnames of the devices with those IDs. For example, if you set the hostname on the device to "IS-IS Router 1", the mapping feature uses this name instead of the device's IS-IS system ID in the output of the following commands:

- show isis database
- show isis interface
- show isis neighbor

The **no** form of the command disables IS-IS name capability on a device.

Examples

The following example disables IS-IS name mapping.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no hostname
```

The following example re-enables IS-IS name mapping.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hostname
```

ike-profile

Configures the IKE profile attached with the IPsec profile.

Syntax

ike-profile *ike-profile-name*

no ike-profile *ike-profile-name*

Parameters

ike-profile-name

Specifies the IKE profile name attached with the IPsec profile.

Modes

IPsec profile configuration mode

Usage Guidelines

no

Examples

The following example configures the IKE profile attached with IPsec profile.

```
device(config)# ipsec profile brocade
device(config-ipsec-profile-brocade)# ike-profile red
```

History

Release version	Command history
05.8.00	This command was introduced.

ikev2 auth-proposal

Creates an Internet Key Exchange version 2 (IKEv2) authentication proposal and enters configuration mode for the proposal.

Syntax

ikev2 auth-proposal *auth-name*

no ikev2 auth-proposal *auth-name*

Parameters

auth-name

Specifies the name of an IKEv2 authentication proposal.

Modes

Global configuration mode

Usage Guidelines

An IKEv2 authentication proposal defines the authentication methods used in IKEv2 peer negotiations.

An IKEv2 authentication proposal is activated by attaching it to an IKEv2 profile.

The **no** form of the command removes the IKEv2 authentication proposal configuration.

Examples

The following example shows how to create an IKEv2 authentication proposal named "secure" and enters configuration mode for the proposal.

```
device# configure terminal
device(config)# ikev2 auth-proposal secure
device(config-ike-auth-proposal-secure)#
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 cookie-challenge

Enables the Internet Key Exchange version 2 (IKEv2) cookie challenge option.

Syntax

cookie-challenge *number*

no cookie-challenge *number*

Command Default

By default, this command is disabled.

Parameters

number

Specifies the maximum number of Security Associations (SA) supported. The maximum number of SAs supported are from 1 through 2000.

Modes

Global configuration mode.

Usage Guidelines

The command is enabled only when the maximum number of half-open IKE SAs go beyond the configured cookie challenge number.

The **no** form of the command disables the cookie challenge number.

Examples

The following example configures an IKEv2 cookie challenge.

```
device(config)# ikev2 cookie-challenge 5
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 dhgroup

Configures the group used for Diffie-Hellman (DH) negotiations.

Syntax

ikev2 dhgroup { 1 } { 2 } { 5 } { 14 } { 15 } { 16 } { 19 } { 20 } { 24 }

Parameters

1
Specifies the 768-bit DH group.

2
Specifies the 1024-bit DH group.

5
Specifies the1536-bit DH group.

14
Specifies the 2048-bit DH group.

15
Specifies the 3072-bit DH group.

16
Specifies the 4096-bit DH group.

19
Specifies the 256-bit elliptic curve DH (ECDH) group.

20
Specifies the 384-bit ECDH group.

24
Specifies the 2048-bit DH/SA group.

Modes

IKEv2 proposal configuration mode.

Examples

The following example configures the group used for Diffie-Hellman (DH) negotiations.

```
device(config)# ikev2-proposal
device(config-ikev2-proposal)# ikev2 dhgroup 20
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 exchange-max-time

Configures the maximum setup time for Internet Key Exchange version 2 (IKEv2) message exchange.

Syntax

ikev2 exchange-max-time *seconds*

no ikev2 exchange-max-time *seconds*

Command Default

The default value is 30 seconds.

Parameters

seconds

Specifies the maximum setup time in seconds. The time range is from 1 through 300 seconds.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command resets the maximum setup time to the default value.

Examples

The following example sets the maximum setup time for IKEv2 message exchange to 50 seconds.

```
device# configure terminal
device(config)# ikev2 exchange-max-time 50
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 http-url-cert

Configures the HTTP certification support.

Syntax

ikev2 http-url-cert

no ikev2 http-url-cert

Command Default

By default, this command is disabled.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command removes the configured HTTP certification support.

Examples

The following example configures HTTP certification support.

```
device(config)# ikev2 http-url-cert
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 limit

Configures limits for the number of Internet Key Exchange version 2 (IKEv2) security association (SA) sessions.

Syntax

ikev2 limit { **max-in-negotiation-sa** *limit* | **max-sa limit** *limit* }

no ikev2 limit { **max-in-negotiation-sa** *limit* | **max-sa limit** *limit* }

Command Default

The default limit (for each type of SA session) is 256.

Parameters

max-in-negotiation-sa *limit*

Limits the total number of in-negotiation IKEv2 SA sessions. The range is from 1 through 256.

max-sa *limit*

Limits the total number of IKEv2 SA sessions. The range is from 1 through 256.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command returns the specified SA session limit to the default value.

Examples

The following example shows how to limit the maximum number of in-negotiation IKEv2 SA sessions to 10.

```
device# configure terminal
device(config)# ikev2 limit max-in-negotiation-sa 10
```

The following example shows how to limit the maximum number of IKEv2 SA sessions to 200.

```
device# configure terminal
device(config)# ikev2 limit max-sa 200
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 nat-enable

Globally enables IP security (IPsec) over Network Address Translation (NAT).

Syntax

ikev2 nat-enable

no ikev2 nat-enable

Command Default

IPsec over NAT is disabled.

Modes

Global configuration mode

Usage Guidelines

Before configuring this command, ensure that a NAT device is located between two Internet Key Exchange (IKE) peers or one of the IKE peers must support NAT functionality to address the change of the IP/TCP header in packets. When IPsec over NAT is enabled, the negotiation of NAT Traversal (NAT-T) between the IKE peers is started and if the negotiation is successful, all encapsulating security payload (ESP) packets sent over the tunnel are encapsulated in the UDP header.

The **no** form of this command disables the IPsec tunnels and the IKE exchange is renegotiated without NAT-T.

NOTE
The **ikev2 nat-enable** command is supported only by Brocade MLXe Series devices.

Examples

The following example globally enables IPsec over NAT.

```
device# configure terminal
device(config)# ikev2 nat-enable
```

History

Release version	Command history
5.9.00a	This command was introduced.

ikev2 nat-keepalive

Configures a time interval during which NAT keepalive messages are sent when the IP security (IPsec) over Network Address Translation (NAT) feature is enabled.

Syntax

ikev2 nat-keepalive [*time*]

no ikev2 nat-keepalive [*time*]

Command Default

The default is 5 seconds.

Parameters

time

Time interval, in seconds, during which NAT keep-alive messages are sent. The range is from 1 through 3600 seconds. A value of 0 disables the keepalive feature.

Modes

Global configuration mode

Usage Guidelines

NOTE
The **ikev2 nat-keepalive** command is supported only by Brocade MLXe Series devices.

This command is used in conjunction with the **ikev2 nat-enable** command that enables IPsec over NAT. The keepalive messages are sent periodically to keep the NAT mappings running.

The **no** form of this command resets the keepalive interval to 5 seconds.

Examples

The following example globally enables IPsec over NAT and sets the keepalive interval to 10 seconds.

```
device# configure terminal
device(config)# ikev2 nat-enable
device(config)# ikev2 nat-keepalive 10
```

History

Release version	Command history
5.9.00a	This command was introduced.

ikev2 policy

Creates an Internet Key Exchange version 2 (IKEv2) policy and enters IKEv2 policy configuration mode.

Syntax

ikev2 policy *name*

no ikev2 policy *name*

Command Default

The default IKEv2 policy is **def-ike-policy**.

Parameters

name

Specifies the name of an IKEv2 policy.

Modes

Global configuration mode

Usage Guidelines

Use the **ikev2 policy** command to configure any additional IKEv2 policies that you need.

The **no** form of the command removes any IKEv2 policy configuration other than the default IKEv2 policy.

The default IKEv2 policy cannot be removed.

Only one IKEv2 policy can be selected for a local endpoint (single IPv4 or IPv6 address). Multiple IKEv2 policies selected for the same IP address is invalid.

When multiple matching policies are identified during IKEv2 negotiations, the most recently created matching policy is used.

Examples

The following example creates an IKEv2 policy named test_policy1.

```
device# configure terminal
device(config)# ikev2 policy test_policy1
device(config-ike-policy-test_policy1)#
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 profile

Configures the specified IKEv2 profile and gives you the option of identifying the local endpoint of the tunnel. This command supports IPsec IPv4 and IPv6.

Syntax

ikev2 profile { *name*[**local-identifier**{**address** [*ipv4-address* |*ipv6-address*]][**dn***dn-string*]][**fqdn***fqdn-string*]][**key-id***key-id string*]][**email***email-string*][**remote-identifieraddress** *ipv4-address* |*ipv6-address*|**dn***dn-string*|**fqdn***fqdn-string*| **key-id***key-id string*|**email***email-string*]

[**match identitylocaladdress**[*ipv4-address*|*ipv6-address*|**dn***dn-string*|**fqdn***fqdn-string*| **key-id***key-id string*|**email***email-string*]

no ikev2 profile { *name*[**local-identifieraddress** *ipv4-address* |*ipv6-address*|**dn***dn-string*|**fqdn***fqdn-string*| **key-id***key-id string*| **email***email-string*]

Command Default

This command is not configured.

Parameters

name

Specifies the IKEv2 profile name.

local-identifier

(Optional) Identifies the local endpoint of the tunnel. You can identify the endpoint using the IP address, distinguished name (dn), fully qualified domain name (fqdn), key identifier (key-id), or email.

address[*ipv4-address*|*ipv6-address*]

Identifies the local endpoint of the tunnel using the IPv4 or IPv6 IP address.

dn*string*

Identifies the local endpoint of the tunnel using the LDAP distinguished name.

fqdn*string*

Identifies the local endpoint of the tunnel using the fully qualified domain name.

key-id*string*

Identifies the local endpoint of the tunnel using the key identifier (ID).

email*string*

Identifies the local endpoint of the tunnel using the email address.

remote-identifier

(Optional) Identifies the remote endpoint of the tunnel. You can identify the endpoint using the IP address, distinguished name (dn), fully qualified domain name (fqdn), key identifier (key-id), or email.

address[*ipv4-address*|*ipv6-address*]

Identifies the remote endpoint of the tunnel using the IPv4 or IPv6 IP address.

dn*string*

Identifies the remote endpoint of the tunnel using the LDAP distinguished name.

fqdn*string*
Identifies the remote endpoint of the tunnel using the fully qualified domain name.

key-id*string*
Identifies the remote endpoint of the tunnel using the key identifier (ID).

email*string*
Identifies the remote endpoint of the tunnel using the email address.

match identity
(Optional) Causes the IKE profile Peer Authorization Database (PAD) for the peers to be automatically selected based on the identity parameters received by the local or remote endpoints. The parameters you specify are used to select the PAD.

Modes

Global configuration mode.

Usage Guidelines

no

Using the command automatically enters IKEv2 profile configuration mode.

Examples

The following example configures the IKEv2 profile named test1.

```
device(config)# ikev2 profile test1
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00	This command was modified to add support for IPsec IPv6 and to add the local identifier option.

ikev2 proposal

Creates an Internet Key Exchange version 2 (IKEv2) proposal and enters IKEv2 proposal configuration mode.

Syntax

ikev2 proposal *name*

no ikev2 proposal *name*

Command Default

The default IKEv2 proposal is **def-ike-proposal**.

Parameters

name

Specifies the name of an IKEv2 proposal.

Modes

Global configuration mode

Usage Guidelines

An IKEv2 proposal defines a set of algorithms that are used in IKEv2 peer negotiations.

The **no** form of the command removes any IKEv2 proposal configuration other than the default IKEv2 proposal configuration.

Examples

The following example shows how to create an IKEv2 proposal named test_proposal1.

```
device# configure terminal
device(config)# ikev2 proposal test_proposal1
device(config-ike-proposal-test_proposal1)#
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 retransmit-interval

Configures the delay time for resending Internet Key Exchange version 2 (IKEv2) messages.

Syntax

ikev2 retransmit-interval *time*

no ikev2 retransmit-interval *time*

Command Default

The default delay time is 5 seconds.

Parameters

time

Specifies the delay time in seconds. The time ranges from 1 through 60.

Modes

Global configuration mode

Usage Guidelines

The retransmit interval increases exponentially.

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

Examples

The following example show how to configure the delay time for resending IKEv2 messages to 20 seconds.

```
device# configure terminal
device(config)# ikev2 retransmit-interval 20
```

History

Release version	Command history
5.8.00	This command was introduced.

ikev2 retry-count

Configures the maximum number of attempts to retransmit an Internet Key Exchange version 2 (IKEv2) message.

Syntax

ikev2 retry-count *number*

no ikev2 retry-count *number*

Command Default

The default number of attempts is 5.

Parameters

number

Specifies the maximum number of attempts to retransmit an IKE message. The range is from 1 through 25.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the retry count to the default value.

Examples

The following example shows how to configure the number of retry attempts for transmitting an IKEv2 message to 8.

```
device# configure terminal
device(config)# ikev2 retry-count 8
```

History

Release version	Command history
5.8.00	This command was introduced.

ike-profile

Configures the IKE profile attached with the IPsec profile.

Syntax

ike-profile *ike-profile-name*

no ike-profile *ike-profile-name*

Parameters

ike-profile-name

Specifies the IKE profile name attached with the IPsec profile.

Modes

IPsec profile configuration mode

Usage Guidelines

no

Examples

The following example configures the IKE profile attached with IPsec profile.

```
device(config)# ipsec profile brocade
device(config-ipsec-profile-brocade)# ike-profile red
```

History

Release version	Command history
05.8.00	This command was introduced.

include-port

Adds ports to the VSRP.

Syntax

include-port ethernet *slot/port* [**to** *slot/port* | [**ethernet** *slot/port* **to** *slot/port* | **ethernet** *slot/port*]...]

no include-port ethernet *slot/port* [**to** *slot/port* | [**ethernet** *slot/port* **to** *slot/port* | **ethernet** *slot/port*]...]

Command Default

By default, all the ports on which you configure a VRID are interfaces for the VRID.

Parameters

ethernet *slot/port*

Adds the Ethernet interface to the VRID.

to *slot/port*

Adds a range of Ethernet interfaces to the VRID.

Modes

VSRP VRID configuration mode

Usage Guidelines

Removing a port is useful because there is no risk of a loop occurring, such as when the port is attached directly to an end host and you plan to use a port in a metro ring.

When a port is removed from VSRP, the port remains in the VLAN but its forwarding state is not controlled by VSRP.

The **no** form of the command removes the ports from VSRP.

Examples

The following example shows how to remove a port from the VRID.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet /1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# no include-port ethernet 1/2
```

ingress-tunnel-accounting

Excludes the Ethernet header (14 bytes) and Ethernet overhead (20 bytes) and CRC overhead (four bytes) when collecting byte statistics. In other words, it counts only the size of the MPLS packet.

Syntax

ingress-tunnel-accounting exclude-ethernet-overhead

no ingress-tunnel-accounting exclude-ethernet-overhead

Command Default

None.

Modes

MPLS policy configuration mode

Usage Guidelines

The operation of the command, based on the operator input, can be defined as 'y' - the configuration change is done and the counters are cleared, or 'n' - the configuration change is not done and the counters are not cleared.

The command **no ingress-tunnel-accounting exclude-ethernet-overhead** disables only the exclude-ethernet-overhead option. To disable ingress-tunnel-accounting itself, enter the command **no ingress-tunnel-accounting**.
exclude-ethernet-overheadexclude-ethernet-overhead

History

Release version	Command history
5.5.00	This command was modified to enforce the clearing of counters when **exclude-ethernet-overhead** mode is changed, a confirmation message is added to the command and on execution, the command clears the counters.
5.6.00	This command modified the **exclude-ethernet-overhead** option, lets the operator exclude the Ethernet header and Ethernet overhead and CRC overhead when collecting the byte statistics.

initial-contact-payload

Configures sending an initial contact message to a peer for an Internet Key Exchange version 2 (IKEv2) profile.

Syntax

initial-contact-payload

no initial-contact-payload

Command Default

No initial contact message is sent to a peer for an IKEv2 profile.

Modes

IKEv2 profile configuration mode

Usage Guidelines

The initial contact message is sent to ensure that old security associations (SAs) on the peer are deleted. When a device reboots, peers may have security associations (SAs) that are no longer valid. The initial contact message ensures that any old SAs on the peer are deleted.

The **no** form of the command disables initial contact messages from being sent to a peer for an IKEv2 profile.

Examples

The following example enables sending an initial contact message to a peer for an IKEv2 profile named ikev2_profile1.

```
device# configure terminal
device(config)# ikev2 profile ikev2_profile1
device(config-ike-profile-ikev2_profile1)# initial-contact-payload
```

initial-ttl

Configures the Hello packet time to live (TTL) (the number of hops a Hello message can traverse after leaving the device and before the Hello message is dropped).

Syntax

initial-ttl *number*

no initial-ttl *number*

Command Default

The default TTL is 2.

Parameters

number

Specifies the number of hops a Hello message can traverse after leaving the device and before the Hello message is dropped. The range is from 1 through 255. The default value is 2.

Modes

VSRP VRID configuration mode

Usage Guidelines

When a VSRP device (master or backup) sends a VSRP Hello packet, the device subtracts one from the TTL. Thus, if the TTL is 2, the device that originates the Hello packet sends it out with a TTL of 1. Each subsequent device that receives the packet also subtracts one from the packet TTL. When the packet has a TTL of 1, the receiving device subtracts 1 and then drops the packet because the TTL is zero.

A metro ring counts as one hop, regardless of the number of nodes in the ring.

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

Examples

The following examples sets the TTL to 5.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vsrp-1)# initial-ttl 5
```

In-label

Specifies the label that is received in the packets and used to identify the static transit LSP in the router. This, in turn, decides where the next hop will be based on the "next-hop" configuration.

Syntax

in-label *value*

no in-label *value*

Parameters

value Represents the label received in the MPLS header in the packets from upstream. Acceptable ranges for the parameter include Static label min-value and Static label max-value. The value must not exceed the static label range configured on the router.

Modes

MPLS-transit LSP sub-configuration mode.

Usage Guidelines

Examples

The following example displays the **in-label** command:

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# static-transit t1
device(config-mpls-static-transit-t1)# in-label 16
```

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

Command Default

This option is disabled.

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.

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

Examples

This example configures the device to compare MEDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# install-igp-cost
```

integrity

Configures an integrity algorithm for an Internet Key Exchange version 2 (IKEv2) proposal.

Syntax

integrity { **sha256** | **sha384** }

no integrity { **sha256** | **sha384** }

Command Default

The default integrity algorithm is SHA-384.

Parameters

sha256

Specifies SHA-2 family 256-bit (hash message authentication code (HMAC) variant) as the hash algorithm.

sha384

Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.

Modes

IKEv2 proposal configuration mode

Usage Guidelines

Multiple integrity algorithms may be configured for an IKEv2 proposal.

When only one integrity algorithm is configured for an IKEv2 proposal, removing it restores the default configuration.

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

Examples

The following example shows how to configure the integrity algorithm SHA-256 for an IKEv2 proposal name ikev2_proposal.

```
device(config)# ikev2 proposal ikev2_proposal
device(config-ikev2-proposal-ikev2_proposal)# integrity sha256
```

History

Release version	Command history
05.8.00	This command was introduced.

ip

Configures the IP address used in the certificate for the PKI entity.

Syntax

ip *ip-address*

no ip *ip-address*

Parameters

ip-address

Specifies the IP address for the PKI entity.

Modes

PKI entity configuration mode.

Usage Guidelines

no

Examples

The following example configures the IP address for the PKI entity.

```
device(config)# pki entity brocade
device(config-pki-entity-brocade)# ip 10.10.20.1
```

History

Release version	Command history
5.8.00	This command was introduced.

ip access-group

Applies rules specified in an IPv4 access control list (ACL) to traffic entering or exiting an interface.

Syntax

ip access-group { *acl-num* | *acl-name* } { **in** | **out** }

no ip access-group { *acl-num* | *acl-name* } { **in** | **out** }

ip access-group { *acl-num* | *acl-name* } **in** [**ethernet** *slot* **/** *port* ...] [**ethernet** *slot* **/** *port* **to ethernet** *slot* **/** *port* ...]

no ip access-group { *acl-num* | *acl-name* } **in** [**ethernet** *slot* **/** *port* ...] [**ethernet** *slot* **/** *port* **to ethernet** *slot* **/** *port* ...]

Command Default

ACLs are not applied to interfaces.

Parameters

acl-num
: Specifies an ACL number. You can specify from 1 through 99 for standard ACLs and from 100 through 199 for extended ACLs.

acl-name
: Specifies a valid ACL name.

in
: Applies the ACL to inbound traffic on the port.

ethernet *slot* **/** *port*
: Specifies the Ethernet interface from which the packets are coming.

to *slot* **/** *port*
: Specifies the range of Ethernet interfaces from which the packets are coming.

out
: Applies the ACL to outbound traffic on the port.

Modes

Interface subtype configuration modes

Usage Guidelines

To apply an IPv4 ACL name that contains spaces, enclose the name in quotation marks (for example, **ip access-group standard "ACL for Net1" in**).

Through a virtual routing interface, you have the following options:

- (Default) Apply an ACL to all ports of the VLAN.

- One or both of the following options:
  - Apply an ACL to specified ports.
  - Apply an ACL to one or more ranges of ports.

To remove an ACL from an interface, use one of the **no** forms of this command.

Examples

The following example creates a named standard IPv4 ACL, defines rules in the ACL, and applies it on an ethernet interface in the ingress direction:

```
device# configure terminal
device(config)# ip access-list standard Net1
device(config-std-nacl-Net1)# deny host 10.157.22.26
device(config-std-nacl-Net1)# deny 10.157.29.12
device(config-std-nacl-Net1)# deny host IPHost1
device(config-std-nacl-Net1)# permit any
device(config-std-nacl-Net1)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group Net1 in
```

The following example creates a named extended IPv4 ACL, defines rules in the ACL, and applies it on an ethernet interface in the ingress direction:

```
device# configure terminal
device(config)# ip access-list extended "block Telnet"
device(config-ext-nacl-block telnet)# deny tcp host 10.157.22.26 any eq telnet
device(config-ext-nacl-block telnet)# permit ip any any
device(config-ext-nacl-block telnet)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group "block Telnet" in
```

The following example configures port-based VLAN 10, adds ports 1/1 through 2/12 to the VLAN, and then adds virtual routing interface 1 to the VLAN.

The commands following the first line-break configure a standard numbered IPv4 ACL , using the **access-list** command. (You can also use the**ip access list** { **standard** | **extended** } command.)

The commands following the second line-break apply the ACL, in an ingress direction, to a subset of the ports associated with virtual interface 1 and to outgoing traffic on all ports.

```
device# configure terminal
device(config)# vlan 10 name IP-subnet-vlan
device(config-vlan-10)# untag ethernet 1/1 to 1/20 ethernet 2/1 to 2/12
device(config-vlan-10)# router-interface ve 1
device(config-vlan-10)# exit

device(config)# access-list 1 deny host 10.157.22.26
device(config)# access-list 1 deny 10.157.29.12
device(config)# access-list 1 deny host IPHost1
device(config)# access-list 1 permit any

device(config)# interface ve 1
device(config-vif-1)# ip access-group 1 in ethernet 1/1 ethernet 1/3 ethernet 2/1 to 2/4
device(config-vif-1)# ip access-group 1 out
```

ip access-group enable-deny-logging

Running this command on an interface is one of the conditions for enabling logging of traffic denied by IPv4 ACLs applied to the interface. The other condition is the inclusion of the **log** parameter in rules within such ACLs.

Syntax

ip access-group enable-deny-logging [**hw-drop**]

no ip access-group enable-deny-logging [**hw-drop**]

Command Default

Deny-logging for IPv4 ACLs is disabled.

Parameters

hw-drop

Specifies that IPv4 ACL-log packets be dropped in hardware, which reduces CPU load.

Modes

Interface subtype configuration modes

Usage Guidelines

When this command is implemented with the **hw-drop** option, packet-counts of denied traffic will include only the first packet in each time cycle.

Deny-logging is supported for inbound ACLs only.

Deny-logging generates Syslog entries only. No SNMP traps are issued.

VPLS, VLL, and VLL-local endpoints do not support the **ip access-group enable-deny-logging** command.

On Brocade NetIron CES Series and Brocade NetIron CER Series devices, deny-logging takes precedence over ACL accounting. If the **ip access-group enable-deny-logging** command is configured on an interface, and both **enable-accounting** and **log** are present in an ACL rule, statistics for that rule are not collected. The output of the **show access-list accounting** command will indicate that logging is enabled, and that statistics for that ACL rule are not available.

This command is not needed on management interfaces, which log both **permit** and **deny** rules that contain a **log** keyword.

Implementation of both deny-logging and denied-traffic redirection (**ip access-group redirect-deny-to-interf**) on an interface can affect denied-traffic forwarding. For rules that contain the log keyword, deny-logging prevents denied-traffic redirection .

To disable IPv4 ACL deny-logging on an interface, use the **no ip access-group enable-deny-logging** command. You do not have to remove **log** parameters from ACLs and re-apply the ACLs.

To disable the **hw-drop** option, use the **no ip access-group enable-deny-logging hw-drop** command.

Examples

The following example implements IPv4 ACL deny-logging on an interface—for applied ACLs that contain rules with **log** parameters.

```
device# configure terminal
device(config)# interface ethernet 5/1
device(config-if-e1000-5/1)# ip access-group enable-deny-logging
```

ip access-group enable-permit-logging

Running this command on an interface is one of the conditions for enabling logging of traffic permitted by IPv4 ACLs applied to the interface. The other condition is the inclusion of the **log** parameter in rules within such ACLs.

Syntax

ip access-group enable-permit-logging [**selective**]

no ip access-group enable-permit-logging [**selective**]

Command Default

Permit-logging for IPv4 ACLs is disabled.

Parameters

selective

Configures logging of permitted traffic to include only the first packet in each time cycle.

Modes

Interface subtype configuration modes

Usage Guidelines

To avoid high CPU usage under permit log generation, include the **selective** keyword.

Logging is supported for inbound ACLs only.

Logging generates Syslog entries only. No SNMP traps are issued.

VPLS, VLL, and VLL-local endpoints do not support logging.

On Brocade NetIron CES Series and Brocade NetIron CER Series devices, logging takes precedence over ACL accounting. If the **ip access-group enable-permit-logging** command is configured on an interface, and both **enable-accounting** and **log** are present in an ACL rule, statistics for that rule are not collected. The output of the **show access-list accounting** command will indicate that logging is enabled, and that statistics for that ACL rule are not available.

This command is not needed on management interfaces, which log both **permit** and **deny** rules that contain a **log** keyword.

To disable IPv4 ACL permit-logging on an interface, use the **no ip access-group enable-permit-logging** form of this command. You do not have to remove **log** parameters from ACLs and re-apply the ACLs.

To disable the **selective** option, use the **no ip access-group enable-permit-logging selective** command.

Examples

The following example implements IPv4 ACL permit-logging on an interface—for applied ACLs that contain rules with **log** parameters.

```
device# configure terminal
device(config)# interface ethernet 5/1
device(config-if-e1000-5/1)# ip access-group enable-permit-logging
```

History

Release	Command History
6.0.00a	This command was introduced.

ip access-group redirect-deny-to-interf

Redirects traffic with **deny** IPv4 ACL matches to an interface that you specify.

Syntax

ip access-group redirect-deny-to-interf *slot* **/** *port*

no ip access-group redirect-deny-to-interf *slot* **/** *port*

Command Default

No redirect is defined.

Parameters

slot **/** *port*

Specifies the interface to which denied traffic is redirected.

Modes

Interface subtype configuration modes

Usage Guidelines

Denied-traffic redirection is supported for inbound ACLs only.

VPLS, VLL, and VLL-local endpoints do not support the **ip access-group redirect-deny-to-interf** command.

Implementation of both deny-logging (**ip access-group enable-deny-logging**) and denied-traffic redirection on an interface can affect denied-traffic redirection. For rules that contain the log keyword, deny-logging prevents denied-traffic redirection.

To disable denied-traffic redirection, use the **no** form of this command (with *slot* **/** *port*).

Examples

The following example implements ACL denied-traffic redirection on an interface

```
device# configure terminal
device(config)# interface ethernet 5/2
device(config-if-e1000-5/2)# ip access-group redirect-deny-to-interf
```

ip access-group ve-traffic

Enables filtering of traffic switched within a virtual routing interface.

Syntax

ip access-group ve-traffic

no ip access-group ve-traffic

Command Default

ACLs do not filter traffic switched from one port to another within a virtual routing interface.

Modes

Virtual-routing interface mode

Usage Guidelines

This command does not affect ACLs applied to outbound traffic.

The **no** form of this command disables filtering of traffic switched within a virtual routing interface.

Examples

The first phase of the following example configures port-based VLAN 10, adds ports 1/1 through 2/12 to the VLAN, and then adds virtual routing interface 1 to the VLAN.

```
device# configure terminal
device(config)# vlan 10 name IP-subnet-vlan
device(config-vlan-10)# untag ethernet 1/1 to 1/20 ethernet 2/1 to 2/12
device(config-vlan-10)# router-interface ve 1
device(config-vlan-10)# exit
```

The second phase of the example configures a standard numbered IPv4 ACL, using the **access-list** command. (You can also use the **ip access list** and [**sequence**] { **permit** | **deny** } commands.)

```
device(config)# access-list 1 deny host 10.157.22.26
device(config)# access-list 1 deny 10.157.29.12
device(config)# access-list 1 deny host IPHost1
device(config)# access-list 1 permit any
```

The third phase of the example enables filtering of traffic switched within a virtual routing interface. It then applies the ACL, in an ingress direction, to a subset of the ports associated with virtual interface 1.

```
device(config)# interface ve 1
device(config-vif-1)# ip access-group ve-traffic
device(config-vif-1)# ip access-group 1 in ethernet 1/1 ethernet 1/3 ethernet 2/1 to 2/4
```

ip access-list

Creates a named or numbered IPv4 standard or extended access 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** } { *acl-num* | *acl-name* }

no ip access-list { **standard** | **extended** } { *acl-num* | *acl-name* }

Command Default

No IPv4 named or numbered ACLs are defined. However, you can also create numbered IPv4 ACLs, using the **access-list** command.

Parameters

standard

Creates a standard access list. Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified address.

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.

acl-num

Specifies the ACL number for a standard or extended access list. The value can be from 1 through 99 for standard IPv4 ACLs and from 100 through 199 for extended IPv4 ACLs.

acl-name

Specifies a unique IPv4 ACL name. The name can be up to 255 characters, and must begin with an alphabetic character. If the name contains spaces, put it within quotation marks. Otherwise, no special characters are allowed, except for underscores and hyphens.

Modes

Global configuration mode

Usage Guidelines

An IPv4 ACL name must be unique among standard and extended ACL types.

After you create a named ACL, enter one or more [**sequence**] { **permit** | **deny** } commands to create filtering rules for that ACL.

An IPv4 ACL starts functioning only after if is applied to an interface using the **ip access-group** command.

The system supports the following IPv4 ACL resources:

- IPv4 numbered standard ACLs—99
- IPv4 numbered extended ACLs—100

- IPv4 named standard ACLs—100
- IPv4 named extended ACLs—500
- Maximum filter-rules per IPv4 or IPv6 ACL—4096. You can change the maximum up to 102400 by using the **system-max ip-filter-sys** command.

The **no** form of this command deletes the ACL. You can delete an IPv4 ACL only after you first remove it from all interfaces to which it is applied, using the **no ip access-group** command.

Examples

The following example creates a standard, named IPv4 ACL, defines rules in it, and applies it to an ethernet interface.

```
device(config)# ip access-list standard Net1
device(config-std-nacl-Net1)# deny host 10.157.22.26
device(config-std-nacl-Net1)# deny 10.157.29.12
device(config-std-nacl-Net1)# deny host IPHost1
device(config-std-nacl-Net1)# permit any
device(config-std-nacl-Net1)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group Net1 in
```

The following example creates an extended, named IPv4 ACL, defines rules in it, and applies it to an ethernet interface, in the ingress direction.

```
device(config)# ip access-list extended "block Telnet"
device(config-ext-nacl-block telnet)# deny tcp host 10.157.22.26 any eq telnet
device(config-ext-nacl-block telnet)# permit ip any any
device(config-ext-nacl-block telnet)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group "block Telnet" in
```

The following example creates an extended, numbered IPv4 ACL and defines rules in it.

```
device# configure terminal
device(config)# ip access-list extended 101
device(config-ext-nacl-)# seq 30 deny udp 19.1.2.0 0.0.0.255 eq 2023 20.1.2.0 0.0.0.255 eq 2025 dscp-
mapping 23
device(config-ext-nacl-)# permit 12 host 098.096.31.10 any
device(config-ext-nacl-)# deny tcp  host 098.092.12.10 131.21.12.0/24 syn
device(config-ext-nacl-)# deny 120  host 18.192.112.110 13.2.2.0/24 log
device(config-ext-nacl-)# permit ip any any mirror
```

ip access-list logging-age

Specifies, in minutes, how long the system waits before it sends a message in the Syslog.

Syntax

ip access-list logging-age *minutes*

no ip access-list logging-age *minutes*

Command Default

The default is five minutes.

Parameters

minutes

Specifies, in minutes, how long the system waits before it sends a message in the Syslog. Valid values range from 1 through 10. The default is five minutes.

Modes

Global configuration mode

Usage Guidelines

To reset the default value of five minutes, use the **no** form of this command.

Examples

The following example sets **logging-age** to two minutes.

```
device# configure terminal
device(config)# ip access-list logging-age 2
```

ip allow-src-multicast

Allows packets with multicast addresses as source IP addresses.

Syntax

ip allow-src-multicast [*decimal* | **all**]

no ip allow-src-multicast [*decimal* | **all**]

Command Default

Packets with multicast addresses as source IP addressed are not forwarded.

Parameters

decimal

Specifies the slot number on which multicast addresses as source IP addresses shoud be allowed.

all

Specifies all slots on which multicast addresses as source IP addresses are allowed.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables multicast addresses as source IP addresses. You cannot configure the **ip allow-src-multicast** command along with the **ip allow-src-multicast switched-traffic** command on the same slot.

Examples

The following example allows all multicast addresses as source IP addresses for all traffic and for all slots.

```
device(config)# ip allow-src-multicast all
```

The following example shows allowing multicast IP addresses as source address for a particular slot.

```
device(config)# ip allow-src-multicast 2
```

History

Release version	Command history
5.9.00	This command was introduced.

ip allow-src-multicast switched-traffic

Disables packet drop for switched traffic only.

Syntax

ip allow-src-multicast switched-traffic [*decimal* | **all**]

no ip allow-src-multicast switched-traffic [*decimal* | **all**]

Command Default

Packet drop for switched traffic is enabled.

Parameters

decimal

Specifies the slot number on which the switched traffic should be allowed.

all

Specifies all slots on which switched traffic is allowed.

Modes

Global configuration mode

Usage Guidelines

You cannot configure the **ip allow-src-multicast switched-traffic** command and **ip allow-src-multicast** command on the same slot. The **no** form of this command enables packet drop for switched traffic.

Examples

The following example allows multicast addresses as source IP addresses for switched traffic for a particular slot.

```
device(config)# ip allow-src-multicast switched-traffic 2
```

The following example allows multicast addresses as source IP addresses for switched traffic for all slots.

```
device(config)# ip allow-src-multicast switched-traffic all
```

History

Release version	Command history
5.9.00	This command was introduced.

ip arp-refresh-request-timer

Sets the ARP refresh request timer and enhances the ARP scaling number to 128k.

Syntax

ip arp-refresh-request-timer *num*

Command Default

The default value is 120 seconds.

Parameters

num

Timer setting in seconds. Possible values are 10 through 3600 seconds.

Modes

Global configuration mode.

Usage Guidelines

Use the default value as minimum the value in scaled configuration.

The ARP request timer must be greater than the ARP pending retry timer.

Examples

The following example sets the ARP refresh timer to 240 seconds.

```
device# configure terminal
device(config)# ip arp-refresh-request-timer 240
```

History

Release version	Command history
5.8.00	This command is introduced.

ip host

Maps a hostname to an IP address.

Syntax

ip host *name ip-address*

no ip host *name ip-address*

Command Default

No hostname is mapped to an IP address.

Parameters

name

Specifies a hostname; for example, www.example.com.

ip-address

Specifies an IP address in either IPv4 or IPv6 format.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the specified hostname mapping.

Examples

The following example shows how to map a host named www.example.com to the IPv4 address 192.168.0.25

```
device(config)# ip host www.example.com 192.168.0.25
```

The following example shows how to map a host named www.example.com to the IPv6 address E80::0202:B3FF:FE1E:8329

```
(config)# ip host www.example.com FE80::0202:B3FF:FE1E:8329
```

History

Release version	Command history
5.8.00	This command was introduced.

ip http client connection timeout connect

This command sets the maximum time for the client to wait for the connection to be established while initiating a connection to the HTTP(S) server.

Syntax

ip http client connection timeout connect *seconds*

no ip http client connection timeout connect

Parameters

seconds

Specifies the amount of time in seconds that the client will wait for the connection to be established with the HTTP(S) server. Can be an integer value from 1 to 15. The default value is 5.

Modes

Privileged EXEC mode

Usage Guidelines

no

Examples

The following example sets the time to the default value of 5 seconds.

```
device(config)# no ip http client connection timeout connect
```

The following example sets the time to 12 seconds.

```
device(config)# ip http client connection timeout connect 12
```

History

Release version	Command history
05.9.00	This command was introduced.

ip http client connection timeout idle

This command sets the maximum time for the client to keep the connection to the http(s) server idle before closing the connection.

Syntax

ip http client connection timeout idle [*seconds*]

Parameters

seconds

Specifies the amount of time in seconds that the client will wait for the connection to be established with the http(s) server. Can be an integer value from 1 to 15. The default value is 5.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example sets the time to the default value of 5 seconds.

```
device(config)# ip http client connection timeout idle
```

The following example sets the time to 12 seconds.

```
device(config)# ip http client connection timeout idle 12
```

History

Release version	Command history
05.9.00	This command was introduced.

ip http client source-interface

Configures the source-interface for the HTTP[S] client.

Syntax

ip http client source-interface { **ethernet** | **loopback** | **ve** } *interface-number*

Parameters

interface-number

Specifies the interface number for the source interface of the HTTP(S) client. When the *source-interface* is *ethernet*, the *interface-number* must be in the form *slot/port*. For loopback and logical interfaces, you must use an integer value for *interface-number*.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example configures the source interface (slot 7, port 12) for the HTTP(S) client.

```
device(config)# ip http client source-interface ethernet 7/12
```

The following example configures the loopback interface for the HTTP(S) client.

```
device(config)# ip http client source-interface loopback 1
```

The following example configures the logical interface (2) for the HTTP(S) client.

```
device(config)# ip http client source-interface ve 2
```

History

Release version	Command history
05.9.00	This command was introduced.

ip icmp fast-echo-reply

Configures hardware-assisted Internet Control Message Protocol (ICMP) response generation for the default virtual routing and forwarding (VRF) instance or a specific VRF.

Syntax

ip icmp fast-echo-reply *ip-address* { *network-address* | **any** } [*age-out* | **clear-counters** | **flush**]

no ip icmp fast-echo-reply *ip-address* { *network-address* | **any** } [*age-out* | **clear-counters** | **flush**]

Parameters

ip-address
Specifies the local IP in the router.

any
Specifies any local IP address in the router.

clear-counters
Clears global counters in the management plane.

flush
Flushes all the hardware entries.

network-address
Specifies the source IP address or network from where ICMP originated.

any
Specifies any source IP address.

age-out
Specifies the aging timer in seconds. The range is from 5 through 360 and the default value is 5.

Modes

Global configuration mode

IP VRF configuration mode

Usage Guidelines

no

Examples

The following example shows how to configure hardware-assisted ICMP response generation.

```
device# configure terminal
device(config)# ip icmp fast-echo-reply 10.1.1.10 any 30
```

History

Release version	Command history
5.7.00	This command was introduced.

ip multicast-routing fast-convergence

Enables fast convergence.

Syntax

ip multicast-routing fast-convergence

no ip multicast-routing fast-convergence

Command Default

Fast convergence is disabled.

Modes

Global configuration mode.

Usage Guidelines

When you enable fast convergence, each PIM join is sent immediately, which ensures faster convergence. However, enabling fast convergence also increases the number of PIM messages on the system. In systems with very high number of mcache entries, batching of PIM messages is recommended to reduce the number of periodic messages and for faster convergence.

The **no** form of the command disables fast convergence.

Examples

The following example configures fast convergence.

```
device# configure terminal
device(config)# ip multicast-routing fast-convergence
```

History

Release version	Command history
5.4	This command was introduced.

ip multicast-routing optimization mct-scaling

Enables IPv4 PIM over MCT scaling optimization.

Syntax

ip multicast-routing optimization mct-scaling

no ip multicast-routing optimization mct-scaling

Command Default

PIM over MCT has a scaling limit of 2K mcache (S,G) entries and 512 IGMP entries.

Modes

Global configuration mode.

Usage Guidelines

Apply this command on both MCT peers.

When you enable PIM over MCT scaling optimization, the maximum scaling of mcache entries to 16K entries and IGMP entries to 4K entries.

The **no** form of the command resets the default scaling limits.

Examples

The following example configures MCT scaling optimization.

```
device# configure terminal
device(config)# ip multicast-routing optimization mct-scaling
```

History

Release version	Command history
06.1.00	This command was introduced.

ip match-payload-len

The IP payload length range can be updated on all PPCR of a slot or one PPCR of slot or all PPCR of all slots. The Min and Max value of payload length range are included in comparison.

Syntax

ip match-payload-len slot{ **all** | **slot** *number* } [**ppcr** *ppcr_id*] [**range** *Min Max*]

no ip match-payload-len slot

Command Default

No IP payload length based filtering using ACL is applied to the interface.

Parameters

slot

Slot number.

all

All slots.

range

Payload length range.

min

Minimum of the payload length range.

max

Maximum of the payload length range.

Modes

Interface subtype configuration modes.

Usage Guidelines

To remove IP payload length based filtering using ACL, use the **no** form of this command.

Examples

Configure IP payload length across system

```
device(config)#ip match-payload-len slot all range 700 1000
```

Configure IP payload length on all PPCR on given slot

```
device(config)#ip match-payload-len slot 2 range 800 800
```

Configure IP payload length on selected PPCR

```
device(config)#ip match-payload-len slot 1 ppcr 1 range 0 1000
```

Removing IP payload length configuration from selected PPCR

```
device(config)#no ip match-payload-len slot 2 ppcr 1
```

History

Release version	Command history
6.0.00a	This command was introduced.

ip multicast-routing load-sharing

Enables or disables load distribution among IP ECMP paths.

Syntax

ip multicast-routing load-sharing [**rebalance**]

no ip multicast-routing load-sharing [**rebalance**]

Parameters

rebalance

Specifies that the ECMP load-sharing will be re-balanced for the interface on which the **rebalance** keyword is configured.

Modes

Interface configuration mode.

Examples

To configure Multicast ECMP, use this command in the configuration mode.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip multicast-routing load-sharing
```

To disable load distribution among ECMP IP paths use the **no** form of the command.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# no ip multicast-routing load-sharing
```

The following example configures re-balancing of the load distribution among ECMP IP paths.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip multicast-routing load-sharing rebalance
```

History

Release	Command History
5.5.00	This command was introduced.

ip ospf active

Sets a specific OSPF interface to active.

Syntax

ip ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ip ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPF control packets.

Examples

The following example sets a specific OSPFv2 Ethernet interface to active.

```
device# configure termnial
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf active
```

ip ospf area

Enables OSPFv2 on an interface.

Syntax

ip ospf area *area-id* | *ip-addr*

no ip ospf area

Command Default

Disabled.

Parameters

area-id

Area ID in decimal format. Valid values range from 1 through 2147483647.

ip-addr

Area ID in IP address format.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command disables OSPFv2 on the interface.

Examples

The following example enables a configured OSPFv2 area named 0 on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf area 0
```

ip ospf auth-change-wait-time

Configures authentication-change hold time.

Syntax

ip ospf auth-change-wait-time *wait-time*

no ip ospf auth-change-wait-time

Command Default

Wait time is 300 seconds

Parameters

wait-time

Time before an authentication change takes place. Valid values range from 0 to 14400 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the authentication change hold time for the interface to which you are connected.

OSPFv2 provides graceful authentication change for the following types of authentication changes:

Changing authentication methods from one of the following to another of the following:

- Simple text password
- MD5 authentication
- No authentication

Configuring a new simple text password or MD5 authentication key.

Changing an existing simple text password or MD5 authentication key

The **no** form of the command resets the wait time to the default of 300 seconds.

Examples

The following example sets the wait time to 600 seconds on a specific OSPFv2 Ethernet interface.

```
device# configure termnial
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf auth-change-wait-time 600
```

ip ospf authentication-key

Configures simple password-based authentication for OSPF.

Syntax

ip ospf authentication-key { **0** *password* | **1** *password* | *password* }

no ip ospf authentication-key

Command Default

Authentication is disabled.

Parameters

0 *password*

the key string is not encrypted and is in clear text.

1 *password*

the key string uses proprietary simple cryptographic 2-way algorithm.

password

OSPF processes *password* as a plain text password. OSPF internally encrypts this 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 in clear text.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf authentication-key 0 morningadmin
```

ip ospf bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv2 interface.

Syntax

ip ospf bfd disable

no ip ospf bfd

Command Default

BFD is disabled by default.

Parameters

disable

Disables BFD on the OSPFv2 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated if BFD is also enabled globally using the **bfd all-interfaces** command in OSPF router configuration mode. If BFD is disabled using the **no bfd all-interfaces** 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 a specific OSPF Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf bfd
```

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

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf bfd disable
```

ip ospf cost

Configures cost for a specific interface.

Syntax

ip ospf cost *value*

no ip ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv2 cost on the interface. If the cost is not configured with this command, OSPFv2 calculates the value from the reference and interface bandwidths.

You can modify the cost to differentiate between 100 Mbps, 1 Gbps, and 10 Gbps. The default cost is calculated by dividing 100 million by the bandwidth. For 10 Mbps links, the cost is 10. The cost for 100 Mbps, 1 Gbps, and 10 Gbps links is 1, because the speed of 100 Mbps and 10 Gbps was not in use at the time the OSPF cost formula was devised.

The **no** form of the command disables the configured cost.

Examples

The following example sets the cost to 600 on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf cost 600
```

ip ospf database-filter

Configures filters for different types of outgoing Link State Advertisements (LSAs).

Syntax

ip ospf database-filter all out

ip ospf database-filter all-external { **allow-default out** | **allow-default-and-type-4 out** | **out** }

ip ospf database-filter all-summary-external { **allow-default out** | **allow-default-and-type-4 out** | **out** }

no ip ospf database-filter all out

no ip ospf database-filter all-external

no ip ospf database-filter all-summary-external

Command Default

All filters are disabled.

Parameters

all out
Blocks all LSAs.

all-external
Blocks all external 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-summary-external
Blocks all summary (Type 3) and external (type 5) LSAs.

Modes

Interface subtype configuration mode

Usage Guidelines

By default, the device floods all outbound LSAs on all the OSPFv2 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.

Enter **no ip ospf database-filter** followed by the appropriate operands to disable this configuration.

NOTE
You cannot block LSAs on virtual links and LSA filtering is not supported on sham links.

Examples

To apply a filter to block flooding of all LSAs on a specific OSPF 40-gigabit Ethernet interface:

```
device(config)# interface fortygigabitethernet 101/0/10
device(conf-if-fo-101/0/10)# ip ospf database-filter all-out
```

To apply a filter to block flooding of all LSAs on a specific OSPF virtual Ethernet (VE) interface:

```
device(config)# rbridge-id 178
device(config-rbridge-id-178)# interface ve 24
device(config-Ve-24)# ip ospf database-filter all-out
```

ip ospf dead-interval

Configures the neighbor dead interval, which is the number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ip ospf dead-interval *interval*

no ip ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 2147483647 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 default OSPF timer values of 10 seconds for the hello-interval and 40 seconds for the dead-interval or higher are recommended on Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

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 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf dead-interval 200
```

ip ospf hello-interval

Configures the hello interval, which is the length of time between the transmission of hello packets that this interface sends to neighbor routers.

Syntax

ip ospf hello-interval *interval*

no ip ospf hello-interval

Command Default

The default value is 10 seconds.

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello interval, unless the dead interval is also explicitly configured using the **ip ospf dead-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.
- The default OSPF timer values of 10 seconds for the hello-interval and 40 seconds for the dead-interval or higher are recommended on Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

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 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf hello-interval 50
```

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 MD5_key* **key** *password* }

no ip ospf md5-authentication key-id

Command Default

No authentication.

Parameters

key-activation-wait-time *wait-time*

Sets the time that OSPFv2 waits before activating a new MD5 key. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends use the newly configured MD5 Key. OSPFv2 packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. Valid values range from 0 to 14400 seconds. The default value is 300 seconds.

key-id

Sets MD5 key and OSPFv2 password.

id MD5_key

The *num* is a number between 1 and 255 and identifies the MD5 key that is being used. This parameter is required to differentiate among multiple keys defined on a router. When MD5 is enabled, the *key* is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPFv2 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.

0 *password*

The key string is not encrypted and is in clear text.

1 *password*

The key string uses proprietary simple cryptographic 2-way algorithm.

2 *password*

The key string uses proprietary base64 cryptographic 2-way algorithm (only for Brocade NetIron XMR Series and Brocade NetIron MLX Series devices).

ospf_password

OSPF processes *password* as a plain text password. OSPF internally encrypts this password as if encryption key 2 was specified and shows the encrypted password in the **show running** command output as follows:

```
key 2 $ci1pVT0=
```

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.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf md5-authentication key-activation-wait-time 240
```

ip ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Command Default

Enabled

Modes

Interface subtype configuration mode

Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv2 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The **no** no form of the command disables MTU-match checking on a specific interface.

Examples

The following example disables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# no ip ospf mtu-ignore
```

The following example enables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf mtu-ignore
```

ip ospf network

Configures the network type for the interface. Point-to-point can support unnumbered links, which requires less processing by OSPF.

Syntax

ip ospf network { **broadcast** | **non-broadcast** | **point-to-point** }

no ip ospf network

Command Default

Network type is broadcast.

Parameters

broadcast

Network type is broadcast.

non-broadcast

Network type is non-broadcast. An interface can be configured to send OSPF traffic to its neighbor as unicast packets rather than multicast packets.

point-to-point

Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

On a non-broadcast interface, the devices at either end of the interface must configure non-broadcast interface type and the neighbor IP address. There is no restriction on the number of devices sharing a non-broadcast interface.

To configure an OSPF interface as a non-broadcast interface, the feature must be enabled on a physical interface or a VE, following the **ip ospf area** statement, and then specify the IP address of the neighbor in the OSPF configuration. The non-broadcast interface configuration must be done on the OSPF devices at either end of the link.

The **no** form of the command removes the network-type configuration.

Examples

The following example configures an OSPFv2 point-to-point link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf network point-to-point
```

The following example configures an OSPFv2 broadcast link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf network broadcast
```

ip ospf passive

Sets a specific OSPFv2interface to passive.

Syntax

ip ospf passive

no ip ospf passive

Command Default

All OSPF interfaces are active.

Modes

Interface subtype configuration mode

Usage Guidelines

When you configure an OSPF interface to be passive, that interface does not send or receive OSPF route updates. Since a passive interface does not send or receive route information, the interface is in effect a stub network.

You might want to set an interface to passive mode if:

- You are planning to use the router mostly for debugging purposes.
- The router is a stub and does not route traffic.

The **no** form of the command sets an interface back to active.

Examples

The following example sets a specific OSPFv2 Ethernet interface to passive.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf passive
```

ip ospf priority

Configures priority for designated router (DR) election.

Syntax

ip ospf priority *value*

no ip ospf priority

Command Default

The default value is 1.

Parameters

value

Priority value. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv2 router assigned the highest priority becomes the designated router, and the OSPFv2 router with the second-highest priority becomes the backup router.

If you set the priority to 0, the device does not participate in DR and BDR election.

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 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf priority 10
```

ip ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

Syntax

ip ospf retransmit-interval *interval*

no ip ospf retransmit-interval

Command Default

The interval is 5 seconds.

Parameters

interval

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

Examples

The following example sets the retransmit interval to 8 for all OSPFv2 devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf retransmit-interval 8
```

ip ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv2 to send link-state update packets on the interface to which you are connected.

Syntax

ip ospf transmit-delay *value*

no ip ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

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

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf transmit-delay 25
```

ip rate-limit option-pkt-to-cpu policy-map

Applies rate-limit on IPv4 option packets.

Syntax

ip rate-limit option-pkt-to-cpu policy-map *rate-limit policy*

no ip rate-limit option-pkt-to-cpu policy-map *rate-limit policy*

Command Default

By default this command is disabled.

Parameters

policy-map *rate-limit policy*

Specifies the name of the policy-map.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables rate-limiting on IPv4 option packets.

Create CPU bound rate-limit policy map before applying rate-limiting for option packets.

NOTE

The following warning message is displayed if only some of the cards are supported and few are not supported.

```
Warning: rate-limit config for protocol "option-pkt-to-cpu" is not supported on module
1, 3
```

The following warning message is displayed if none of the cards are supported.

```
Warning: rate-limit config for protocol "option-pkt-to-cpu" is not supported on
available modules. It is only supported on GEN-2 and later modules.
```

Examples

The following example explains how to apply rate-limit for IPv4 option packets.

```
device(config)#ip rate-limit option-pkt-to-cpu policy-map save-cpu-policy
```

History

Release version	Command history
5.8.00	This command was introduced.

ip rate-limit ttl-expired-to-cpu policy-map

Applies rate-limit option on IPv4 ttl packets, if the ttl count is less than or equal to one.

Syntax

ip rate-limit ttl-expired-to-cpu policy-map *rate-limit policy*

no ip rate-limit ttl-expired-to-cpu policy-map *rate-limit policy*

Command Default

By default this command is disabled.

Parameters

policy-map *rate-limit policy*

Specifies the name of the policy-map.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables rate-limit option on IPv4 ttl-expired-to-cpu packets.

Create a CPU bound rate-limit policy map before applying rate-limiting for ttl-expired-to-cpu packets.

NOTE

The following warning message is displayed if only some of the cards are supported and few are not supported.

```
Warning: rate-limit config for protocol "ttl-expired-to-cpu" is not supported on module
1, 3
```

The following warning message is displayed if none of the cards are supported.

```
Warning: rate-limit config for protocol "ttl-expired-to-cpu" is not supported on
available modules. It is only supported on GEN-2 and later modules.
```

Examples

The following example explains how to apply rate-limit option on IPv4 ttl-expired-to-cpu packets.

```
device(config)# ip rate-limit ttl-expired-to-cpu policy-map save-cpu-policy
```

History

Release version	Command history
5.8.00	This command was introduced.

ip receive access-list

Applies an IPv4 ACL as a receive access-control list (rACL).

Syntax

ip receive access-list { **acl-num** | *acl-name* } **sequence** *seq-num* [**policy-map** *policy-map-name* [**strict-acl**]]

no ip receive access-list { **acl-num** | *acl-name* } **sequence** *seq-num* [**policy-map** *policy-map-name* [**strict-acl**]]

Parameters

acl-num* | *acl-name	Specifies, in number or name format, the access-control list to apply to all interfaces within the default VRF, for all CPU-bound traffic.
sequence *seq-num*	Defines the sequence number of the access-control list being applied as a rACL. IPv4 rACL commands are applied in the order of the lowest to the highest sequence numbers. The range of values is from 1 through 200.
policy-map *policy-map-name*	Specifies the name of a policy map. When the **policy-map** option is specified, traffic matching the "permit "clause of the specified IPv4 ACL is rate-limited as defined in the policy map and IPv4 traffic matching the "deny" clause in the IPv4 ACL is permitted without rate limiting.
strict-acl	Specifies that traffic matching the "permit" clause of the specified IPv4 ACL is rate-limited as defined in the policy map and IPv4 traffic matching the "deny" clause in the IPv4 ACL is dropped in the hardware.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the basic command removes the rACL.

The **no** form of the command with both **policy-map** and **strict-acl** options specified, removes the **strict-acl** option: the rACL with **policy-map** remains and traffic matching "deny" clauses starts passing to the CPU.

Examples

The following example applies ACL "101" as a device-level rACL with the sequence number "15".

```
device(config)# ip receive access-list 101 sequence 15
```

The following example applies "acl_stand1" as a device-level rACL with the sequence number "10".

```
device(config)# ip receive access-list acl_stand1 sequence 10
```

The following example removes the **strict-acl** option so that traffic matching "deny" clauses starts passing to the CPU. The rACL "acl_stand1" with the policy map "m1" remains.

```
device(config)# no ip receive access-list acl_stand1 sequence 10 policy-map m1 strict-acl
```

History

Release	Command History
5.6.00	This command was modified to support named rACLs.

ip receive access-list enable-permit-logging

Generates logs of IPv4 packets permitted by receive access-control lists (rACLs) applied at device level.

Syntax

ip receive access-list enable-permit-logging [**selective**]

ip receive access-list enable-permit-logging [**selective**]

Command Default

Logs are not generated for IPv4 packets that are permitted by rACLs.

Parameters

selective

Configures logging of permitted traffic to include only the first packet in each time cycle.

Modes

Global configuration mode

Usage Guidelines

To avoid high CPU usage under permit log generation, include the **selective** keyword.

The **no** form of this command disables the log generation.

NOTE
The **ip receive access-list enable-permit-logging** command is supported only on Brocade NetIron MLX Series and Brocade NetIron XMR Series devices.

Examples

The following example enables IPv4 rACL permit logging on the device.

```
device# configure terminal
device(config)# ip receive access-list enable-permit-logging
```

The following example sets the **ip access-list logging-age** parameter to 8 minutes and—for IPv4 rACLs—configures permit logging on the device as selective.

```
device# configure terminal
device(config)# ip access-list logging-age 7
device(config)# ip receive access-list enable-permit-logging selective
```

History

Release	Command History
6.0.00a	This command was introduced.

ip route bfd

Enables Bidirectional Forwarding Detection (BFD) monitoring for an IP static route.

Syntax

ip route *A.B.C.D/L A.B.C.D* **bfd** [*metric* | **distance** *number* | **name** *name* | **tag** *number*

Command Default

BFD monitoring for an IP static route is not enabled.

Parameters

A.B.C.D/L

Specifies the destination IPv4 address and mask.

A.B.C.D

Specifies the IPv4 address of the next hop.

metric

Specifies the cost metric of the route. Valid values range from 1 through 16. The default is 1.

distance *number*

Specifies the administrative distance of the route. Valid values range from 1 through 255. The default is 1.

name *name*

Specifies the name of the route in ASCII characters.

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

Usage Guidelines

The **no** form of the command removes BFD monitoring from the static route.

Examples

The following example enables BFD route monitoring on an IP static route and sets the cost metric of the route to 8.

```
device# configure terminal
device(config)# ip route 10.1.0.0/24 10.2.0.5 bfd 8
```

The following example enables BFD route monitoring on an IP static route and sets the administrative distance of the route to 60.

```
device# configure terminal
device(config)# ip route 10.0.0.0/24 10.0.0.5 bfd distance 60
```

The following example enables BFD route monitoring on an IP static route and sets the name of the route to “route1”.

```
device# configure terminal
device(config)# ip route 10.0.2.0/24 10.0.3.5 bfd name route1
```

The following example enables BFD route monitoring on an IP static route and sets the tag value of the route to 10.

```
device# configure terminal
device(config)# ip route 10.0.2.0/24 10.0.3.5 bfd tag 10
```

ip route static-bfd

Configures Bidirectional Forwarding Detection (BFD) session parameters for IP static routes.

Syntax

ip route [**vrf** *vrf-name*] **static-bfd** *dest-ip-address source-ip-address* [**interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

no ip route [**vrf** *vrf-name*] **static-bfd** *dest-ip-address source-ip-address*

Command Default

BFD is not configured for an IP static route.

Parameters

vrf *vrf-name*
Specifies the name of a VRF instance.

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.

min-rx *receive-time*
Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000.

multiplier *number*
Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD determines that the connection to that peer is not operational. Valid values range from 3 through 50.

Modes

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 BGP 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.

When Brocade NetIron CER Series or Brocade NetIron CES Series devices are heavily loaded or under stress, BFD sessions may flap if the configured BFD interval is less than 500 milliseconds with a multiplier value of 3.

The **no** form of the command disables BFD monitoring by removing the BFD static neighbor and eliminating the BFD session, while keeping the static route in the route table manager (RTM), and retaining the existing IP traffic route. You only need to specify the destination and source IP address when removing a BFD neighbor.

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
```

ip router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing at the interface level.

Syntax

ip router isis

Command Default

Disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to disable IS-IS routing for the interface.

Examples

The following example enables IS-IS routing for an interface Ethernet.

```
device# configure terminal
device(config)# interface ethernet 1/2
device(config-if-e1000-1/2)# ip router isis
```

ip ssh encryption disable-aes-cbc

Disables the Advanced Encryption Standard - Cipher-Block Chaining (AES-CBC) encryption mode for the Secure Shell (SSH) protocol.

Syntax

ip ssh encryption disable-aes-cbc

no ip ssh encryption disable-aes-cbc

Command Default

If JITC is enabled, only AES-CTR encryption mode is supported and AES-CBC mode is disabled by default. In the standard mode, the AES-CBC encryption mode is enabled.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command enables the AES-CBC encryption mode.

Examples

The following example disables the AES-CBC encryption mode.

```
device# configure terminal
device(config)# ip ssh encryption disable-aes-cbc
```

History

Release version	Command history
5.8.00	This command was introduced.

ip tcp adjust-mss

Configures the TCP MSS value of the IP TCP synchronization packets passing through a router.

Syntax

ip tcp [**adjust-mss** *max-segment-size*]

no ip tcp [**adjust-mss** *max-segment-size*]

Command Default

Configuring the TCP MSS value of the IP TCP synchronization packets is not enabled by default.

Parameters

adjust-mss Specifies the TCP MSS value configuration parameter.

max-segment-size Specifies the maximum segment size in bytes. The range is from 512 - 9158 bytes. Since the range is based on configuration of the IP MTU or GRE Tunnel MTU value, the CLI does not display the configurable range.

Modes

Interface level, and virtual interface (VE) level.

Usage Guidelines

For a GRE tunnel, the **ip tcp adjust-mss** command is supported only on Gen-2 Switch Fabric Modules and later.

Use the **ip tcp adjust-mss** command to modify the TCP MSS value of the IP TCP synchronization packets passing through a router. Please note that the TCP MSS is applicable only for inbound traffic. When you configure the IP MTU value on the same Ethernet interface as the configured TCP MSS value, the software internally modifies the TCP MSS value according to the current IP MTU value so dropped or fragmented packets are avoided. The TCP MSS value is modified based on the IP MTU or GRE tunnel MTU configuration. If the configured TCP MSS value is less than the current IP MTU value or GRE tunnel MTU value, then the software will not modify the TCP MSS value. Refer to the examples below for modifying the TCP MSS value based on the IP MTU configuration or the GRE tunnel MTU configuration.

Modifying the TCP MSS value based on the IP MTU configuration

For example, on ethernet interface 1/1 the TCP MSS is configured to 1400 bytes. If you configure the IP MTU value to 1000 bytes on ethernet interface 1/1, the software internally modifies the TCP MSS value to 960 bytes. The TCP MSS value modification is required by software because the configured TCP MSS value (1400 bytes) is greater than the user configuration of the IP MTU value. The modified value is calculated by subtracting the user configuration from the current IP MTU value - 1000 bytes minus 40 bytes equals 960 bytes.

Modifying the TCP MSS value based on the GRE tunnel MTU configuration

For example, on ethernet interface 1/1 the TCP MSS value is configured to 1400 bytes. The ethernet interface 1/1 is a tunnel source for the GRE tunnel 100. If you configure the GRE tunnel MTU value to 700 bytes on ethernet interface 1/1, the software internally modifies the TCP MSS value to 660 bytes. The TCP MSS value modification is required by software because the configured TCP MSS value (1400 bytes) is greater than the user configuration of the GRE tunnel MTU value. The

modified value is calculated by subtracting the user configuration from the current GRE tunnel MTU value - 700 bytes minus 40 bytes equals 960 bytes.

After configuring the **ip tcp adjust-mss** *max-segment-size* command, and the **ip tcp redirect-gre-tcp-syn** command, the hardware redirects the TCP SYN packets received on interface port 1/1 to the LP software. The LP software adjusts the TCP MSS value in the incoming packet.

The GRE tunnel MTU configuration takes a higher priority over the IP MTU configuration. If the GRE tunnel MTU is not configured, then the IP MTU configuration is used to modify the TCP MSS value. The **ip tcp adjust-mss** *max-segment-size* command can only enabled on the GRE ingress interface. The TCP MSS value is modified only in the source port of the ingress GRE tunnel. The TCP MSS value cannot be modified when the tunnel source port is configured as an IP address port. The **ip tcp adjust-mss** *max-segment-size* command is supported only on an IPv4 interface.

Use the **no** form of the command to disable the TCP MSS value configuration parameter. Backward compatibility is not supported.

NOTE
Configuring the TCP MSS value is supported only on the Brocade NetIron XMR Series and the Brocade NetIron MLX Series platforms.

Examples

The following example configures the TCP MSS value to 1000 bytes.

```
device(config)# interface ethernet 2/1
device(config-if-e10000-2/1)# ip tcp adjust
    adjust-mss   Configure the TCP MSS
device(config-if-e10000-2/1)# ip tcp adjust-mss 10
Error - 10 not between 536 and 1460
device(config-if-e10000-2/1)# ip tcp adjust-mss 1000
device(config-if-e10000-2/1)#
```

Use the **show run interface** command to display the TCP MSS configuration on interface ethernet 2/1.

```
device(config-if-e10000-2/1)# show run interface
interface management 1
ip address x.x.x.x/24
enable
!
interface ethernet 2/1
ip tcp adjust-mss 1000
!
interface ethernet 2/3
ip address x.x.x.x/24
!
interface ethernet 2/4
enable
!
```

History

Release version	Command history
5.7.00	This command was introduced.

ip tcp redirect-gre-tcp-syn

Configures the GRE-based TCP synchronization packets to the CPU when the TCP MSS value is adjusted.

Syntax

ip tcp [**redirect-gre-tcp-syn**]

no ip tcp [**redirect-gre-tcp-syn**]

Command Default

Configuring the GRE based TCP synchronization packets to the CPU is not enabled by default.

Parameters

redirect-gre-tcp-syn

Specifies the GRE-based TCP synchronization packets parameter.

Modes

Global configuration mode.

Usage Guidelines

Use the **ip tcp redirect-gre-tcp-sync** command to optionally redirect the GRE-based TCP synchronization packets to the CPU when the TCP MSS value is adjusted. To redirect the GRE based TCP synchronization packets to the CPU, use the **ip tcp adjust-mss** *max-segment-size* command, and the **ip tcp redirect-gre-tcp-sync** command. To redirect only the IP TCP synchronization packets to the CPU, use**ip tcp adjust-mss** *max-segment-size* command.

After configuring the **ip tcp adjust-mss** command with the *max-segment-size* option, and the **ip tcp redirect-gre-tcp-syn** command, the hardware redirects the TCP SYN packets received on interface port 1/1 to the LP software. The LP software adjusts the TCP MSS value in the incoming packet. For more information on the **ip tcp adjust-mss** *max-segment-size* command, refer to the **ip tcp adjust-mss** command.

Use the **no** form of the command to disable the configuration of the GRE based TCP synchronization packets to the CPU. Backward compatibility is not supported. If the **ip tcp redirect-gre-tcp-sync** command is not configured, the incoming packet still receives the CPU for MAC learning.

You can optionally trap the TCP SYNC packet in a GRE transit router by creating a dummy GRE tunnel in the transit router. For example, port 1/1 is the ingress port and port 1/2 is the egress port for the GRE based TCP SYN packets incoming and outgoing transmission. To trap the TCP SYN packets to the LP CPU on port 1/1, you need to create a dummy GRE tunnel in the configured tunnel source port, either port 1/1 or port 1/2.

NOTE

Configuring the GRE based TCP synchronization packets is supported only on the Brocade NetIron XMR Series and the Brocade NetIron MLX Series platforms.

Examples

The following example configures the GRE based TCP synchronization packets to the CPU on the global interface level.

```
device(config)# ip tcp redirect-gre-tcp-syn ?
redirect-gre-tcp-syn   Control the GRE based TCP Synchronization packets
device(config)# ip tcp redirect-gre-tcp-syn
deviceconfig)#
```

Use the **show running-configuration** command to display the GRE based TCP synchronization packets configuration.

```
device# show running-config
!
hostname dut3
acl-duplication-check
ip multicast-routing
ip tcp redirect-gre-tcp-syn
!
```

History

Release version	Command history
5.7.00	This command was introduced.

ip vrrp auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol (VRRP) interface.

Syntax

ip vrrp auth-type { **no-auth** | **simple-text-auth** *auth-text* }

no ip vrrp auth-type { **no-auth** | **simple-text-auth** *auth-text* }

Command Default

No authentication type is configured on a VRRP interface.

Parameters

no-auth

Configures no authentication on the VRRP interface.

simple-text-auth *auth-text*

Configures a simple text string as a password used for authenticating packets on the interface. The maximum length of the text string is 64 characters.

Modes

Interface configuration mode

Usage Guidelines

If the **no-auth** option is configured, ensure that all interfaces on all devices that support the virtual router ID do not use authentication.

If the **simple-text-auth** option is configured, ensure that all interfaces on all devices that support the virtual router ID are configured to use simple password authentication with the same password.

The **no** form of this command removes the VRRP authentication from the interface.

NOTE

Authentication is not supported by VRRP-Ev3.

Examples

The following example configures no authentication on Ethernet interface 1/6.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp auth-type no-auth
```

The following example configures simple password authentication on Ethernet interface 1/6.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp auth-type simple-text-auth yourpwd
```

ip vrrp vrid

Configures an IPv4 Virtual Router Redundancy Protocol (VRRP) virtual router identifier (VRID).

Syntax

ip vrrp vrid *vrid*

no ip vrrp vrid *vrid*

Command Default

A VRRP VRID does not exist.

Parameters

vrid

Configures a number for the IPv4 VRRP VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that VRRP is enabled globally; otherwise, an error stating "Invalid input..." is displayed as you try to create a VRRP instance.

The **no** form of this command removes the IPv4 VRRP VRID from the configuration.

Examples

The following example configures VRRP virtual router ID 1.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
VRRP router 1 for this interface is activating
```

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 { **no-auth** | **simple-text-auth** *auth-text* | **md5-auth** *auth-text* }

no ip vrrp-extended auth-type { **no-auth** | **simple-text-auth** *auth-text* | **md5-auth** *auth-text* }

Command Default

No authentication is configured for a VRRP-E interface.

Parameters

no-auth

Configures no authentication on the VRRP-E interface.

simple-text-auth *auth-text*

Configures a simple text string as a password used for authenticating packets on the interface. The maximum length of the text string is 64 characters.

md5-auth *auth-text*

Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

Modes

Interface configuration mode

Usage Guidelines

If the **simple-text-auth** option is configured, ensure that all interfaces on all devices that support the virtual router ID are configured to use simple password authentication with the same password.

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.

Use the **show run** command with appropriate parameters to display the encrypted password; use the **enable password-display** command to display the unencrypted password.

If the **no-auth** option is configured, ensure that all interfaces on all devices that support the virtual router ID do not use authentication.

The **no** form of this command removes the VRRP-E authentication from the interface.

NOTE
Authentication is not supported by VRRP-Ev3.

Examples

The following example configures no authentication on Ethernet interface 1/6.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp-extended auth-type no-auth
```

The following example configures simple password authentication on Ethernet interface 1/6.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp-extended auth-type simple-text-auth yourpwd
```

The following example configures MD5 authentication on Ethernet interface 1/6. When MD5 authentication is configured, a syslog message is displayed.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp-extended auth-type md5-auth lyk28d3j

Aug 10 18:17:39 VRRP: Configuration VRRP_CONFIG_MD5_AUTHENTICATION request received
Aug 10 18:17:39 VRRP: Port 1/6, VRID 2 - send advertisement
Ver:3 Type:1 Vrid:2 Pri:240 #IP:1 AuthType:2 Adv:1 Chksum:0x0000
HMAC-MD5 CODE:[00000000000000000000400010]
IpAddr: 10.53.5.1
```

ip vrrp-extended vrid

Configures an IPv4 Virtual Router Redundancy Protocol Extended (VRRP-E) virtual router identifier (VRID).

Syntax

ip vrrp-extended vrid *vrid*

no ip vrrp-extended vrid *vrid*

Command Default

A VRRP-E VRID does not exist.

Parameters

vrid

Configures a number for the IPv4 VRRP-E VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that VRRP-E is enabled globally; otherwise an error stating "Invalid input..." is displayed as you try to create a VRRP-E instance.

The **no** form of this command removes the IPv4 VRRP-E VRID from the configuration.

Examples

The following example configures VRRP-E VRID 1.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.10.1/24
device(config-if-e1000-1/6)# ip vrrp-extended vrid 1
device(config-if-e1000-1/6-vrid-1)# backup priority 50 track-priority 10
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.10.254
device(config-if-e1000-1/6-vrid-1)# activate
```

ip-address

Configures a virtual IP address for a Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) instance.

Syntax

ip-address *ip-address*

no ip-address *ip-address*

Command Default

A virtual IP address is not configured for a VRRP or VRRP-E instance.

Parameters

ip-address

Configures the IP address, in dotted-decimal format.

Modes

VRID interface configuration mode

Usage Guidelines

For VRRP instances, the IP address used for the virtual router must be configured on the device assigned to be the initial VRRP owner device. The same IP address cannot be used on any other VRRP device.

For VRRP-E instances, the IP address used for the virtual router must not be configured on any other device.

The **no** form of this command removes the virtual router IP address.

Examples

The following example configures a virtual IP address for VRID 1 when VRRP is implemented. In this example, the device is configured as the VRRP owner device.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
VRRP router 1 for this interface is activating
```

The following example configures a virtual IP address for VRID 2 when VRRP-E is implemented. In this example, the device is configured as a VRRP backup device and the highest priority device will become the master VRRP device.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.3/24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 110
device(config-if-e1000-1/5-vrid-2)# version 2
device(config-if-e1000-1/5-vrid-2)# ip-address 10.53.5.254
device(config-if-e1000-1/5-vrid-2)# activate
VRRP router 2 for this interface is activating
```

ip-address (VSRP)

Configures the IP address to back up.

Syntax

ip-address *ip-address*

no ip-address *ip-address*

ip address *ip-address*

no ip address *ip-address*

Command Default

The IP address to backup is not configured.

Parameters

ip-address

Configures the IP address to back up.

Modes

VSRP VRID configuration mode

Usage Guidelines

If you are configuring a Layer 3 switch for VSRP, you can specify an IP address to back up. When you specify an IP address, VSRP provides redundancy for the address. This is useful if you want to back up the gateway address used by hosts attached to the VSRP backups. VSRP does not require you to specify an IP address. If you do not specify an IP address, VSRP provides Layer 2 redundancy. If you do specify an IP address, VSRP provides Layer 2 and Layer 3 redundancy.

The VRID IP address must be in the same subnet as a real IP address configured on the VSRP interface, but cannot be the same as a real IP address configured on the interface.

Failover applies to both Layer 2 and Layer 3.

The **no** form of the command removes the configured backup IP address.

Examples

The following example configures the backup IP address.

```
device(config)# vlan 200
device(config-vlan-200)# tagged ethernet 1/1 to 1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# ip-address 10.10.10.1
```

ipsec profile

Creates an IP security (IPsec) profile and enters IPsec profile configuration mode.

Syntax

ipsec profile *name*

no ipsec profile *name*

Command Default

No IPsec profile is configured.

Parameters

name

Specifies the name of an IPsec profile.

Modes

Global configuration mode

Usage Guidelines

An IPsec profile defines parameters for encrypting communications between IPsec peer devices.

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

Examples

The following example shows how to create an IPsec profile named ipsec_profile and enters IPsec profile configuration mode for the profile.

```
device(config)# ipsec profile ipsec_profile
device(config-ipsec-profile-ipsec_profile)#
```

History

Release version	Command history
5.8.00	This command was introduced.

ipsec proposal

Creates an IP security (IPsec) proposal and enters IPsec proposal configuration mode.

Syntax

ipsec proposal *name*

Parameters

name

Specifies the name of an IPsec proposal.

Modes

Global configuration mode

Usage Guidelines

An IPsec proposal defines an encryption algorithm, encapsulation mode, and transform set used to negotiate with a data path peer. An IPsec proposal is activated by attaching it to an IPsec profile.

Examples

The following example creates an IPSec proposal named ipsec_proposal and enters IPsec proposal configuration mode for the proposal .

```
device(config)# ipsec proposal ipsec_proposal
device(config-ipsec-proposal-ipsec_proposal)#
```

History

Release version	Command history
5.8.00	This command was introduced.

ipsec self-sa-learning-enable

Enables learning of self MAC addresses on the device when IP packets are received over an IPsec tunnel.

Syntax

ipsec self-sa-learning-enable

no ipsec self-sa-learning-enable

Command Default

Learning of self MAC addresses is disabled.

Modes

Global configuration mode

Usage Guidelines

When encrypted or decrypted IP packets are looped back to the system (device) for an additional level of encryption or decryption, the packets are not sent to the CPU to learn the self MAC addresses on the device. In this situation, the **ipsec self-sa-learning-enable** command may be used to enable learning of the self MAC addresses on the device for all configured IPsec IPv4 and IPv6 tunnels.

The **no** version of the command disables learning of the self MAC addresses on the device.

The learning of self MAC addresses should be disabled, when it is not needed.

Examples

The following example enables the learning the self MAC addresses for all configured IPsec IPv4 and IPv6 tunnels on the device.

```
device(config)# ipsec self-sa-learning-enable
```

History

Release version	Command history
5.9.00	This command was introduced.

ipv6 access-list

Creates an IPv6 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify. IPv6 ACLs filter traffic only after you apply them to interfaces.

Syntax

ipv6 access-list *acl-name*

no ipv6 access-list *acl-name*

Command Default

There are no default IPv6 ACLs.

Parameters

acl-name

Specifies a unique IPv6 ACL name. The name can be up to 199 consecutive characters (no spaces), and must begin with an alphabetic character. No special characters are allowed, except for underscores and hyphens. The string "test" is a reserved string.

Modes

Global configuration mode

Usage Guidelines

For IPv6 ACLs, only named ACLs are supported.

For IPv6 ACLs, only extended ACLs are supported. Extended ACLs contains rules that permit or deny traffic according to source and destination addresses, port protocol, and other IPv6 frame content.

After you create an IPv6 ACL, use the [**sequence**] { **permit** | **deny** } command to create filtering rules for that ACL.

An IPv6 ACL starts functioning only after it is applied to an interface, using the **ipv6 traffic-filter** command.

The system supports the following IPv6 ACL resources:

- IPv6 named ACLs—1000
- Maximum filter-rules per IPv4 or IPv6 ACL—4096. You can change the maximum up to 102400 by using the **system-max ip-filter-sys** command.

To delete an IPv6 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 the **no ipv6 traffic-filter** command.

Examples

The following example creates an IPv6 ACL, defines within it a rule that blocks all Telnet traffic received from IPv6 host 2000:2382:e0bb::2, and applies the ACL to port 1/1.

```
device# configure terminal
device(config)# ipv6 access-list fdry
device(config-ipv6-access-list-fdry)# deny tcp host 2000:2382:e0bb::2 any eq telnet
device(config-ipv6-access-list-fdry)# permit ipv6 any any
device(config-ipv6-access-list-fdry)# exit
device(config)# interface ethernet 1/1
device(config-if-1/1)# ipv6 traffic-filter fdry in
device(config-if-1/1)# exit
device(config)# write memory
```

The first phase of the following example creates an IPv6 ACL, and defines the following rules within:

- Permit ICMP traffic from hosts in the 2000:2383:e0bb::x network to hosts in the 2001:3782::x network.
- Deny all IPv6 traffic from host 2000:2383:e0ac::2 to host 2000:2383:e0aa:0::24.
- Deny all UDP traffic.
- Permit all packets that are not explicitly denied by the other entries. (Without this entry, the ACL denies all incoming or outgoing IPv6 traffic on the ports to which the ACL is assigned.) Priority-mapping filters IPv6 traffic on the basis of the .1p priority.

```
device# configure terminal
device(config)# ipv6 access-list netw
device(config-ipv6-access-list-netw)# permit icmp 2000:2383:e0bb::/64 2001:3782::/64
device(config-ipv6-access-list-netw)# deny ipv6 host 2000:2383:e0ac::2 host
2000:2383:e0aa:0::24
device(config-ipv6-access-list-netw)# deny udp any any
device(config-ipv6-access-list-netw)# permit ipv6 any any priority-mapping 4
device(config-ipv6-access-list-netw)# exit
```

The second phase of the example applies the ACL to both incoming and outgoing traffic on port 1/2 and to incoming traffic on port 4/3.

```
device(config)# interface ethernet 1/2
device(config-if-1/2)# ipv6 traffic-filter netw in
device(config-if-1/2)# ipv6 traffic-filter netw out
device(config-if-1/2)# exit
device(config)# interface ethernet 4/3
device(config-if-4/3)# ipv6 traffic-filter netw in
device(config-if-4/3)# exit
device(config)# write memory
```

ipv6-address

Configures a virtual IPv6 address for a Virtual Router Redundancy Protocol version 3 (VRRPv3) or VRRP Extended version 3 (VRRP-Ev3) instance.

Syntax

ipv6-address { *ipv6-address* | **auto-gen-link-local** }

no ipv6-address { *ipv6-address* | **auto-gen-link-local** }

Command Default

A virtual IPv6 address is not configured for a VRRPv3 or VRRP-Ev3 instance.

Parameters

ipv6-address

Configures an IPv6 address.

auto-gen-link-local

Automatically generates a virtual IPv6 link-local address for the VRRPv3 instance. Not supported in VRRP-Ev3.

Modes

Virtual routing ID interface configuration mode

Usage Guidelines

For VRRP instances, the IPv6 address used for the virtual router must be configured on the device assigned to be the initial VRRP owner device. The same physical IPv6 address cannot be used on any other VRRP device.

If the **auto-gen-link-local** keyword is entered, a virtual IPv6 link-local address is generated automatically for the specific VRRPv3 instance. The virtual link-local address is carried in VRRPv3 advertisements. A manually configured link-local address takes precedence over the automatically generated address.

NOTE

Automatically generated virtual link-local addresses are not supported for VRRP-Ev3 instances.

The **no** form of the command removes the virtual router IPv6 address. If the **auto-gen-link-local** keyword was active, the automatically generated virtual IPv6 link-local address is removed for the VRRPv3 instance, and subsequent VRRPv3 advertisements will not carry this link-local address.

Examples

The following example configures a virtual IPv6 address for VRID 1 when IPv6 VRRPv3 is implemented. In this example, the device is configured as the VRRPv3 owner device.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ipv6 address fd2b::1/64
device(config-if-e1000-1/6)# ipv6 vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ipv6-address fe80::768e:f8ff:fe2a:0099
device(config-if-e1000-1/6-vrid-1)# ipv6-address fd2b::1
device(config-if-e1000-1/6-vrid-1)# activate
```

The following example automatically configures a virtual IPv6 link-local address for VRID 1 when an IPv6 VRRPv3 instance is activated. In this example, the device is configured as the VRRPv3 owner device.

NOTE

Automatically generated virtual IPv6 link-local addresses are not supported for VRRP-Ev3 instances.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(conf-if-e1000-1/6)# ipv6 address fd2b::1/64
device(conf-if-e1000-1/6)# ipv6 vrrp vrid 1
device(conf-if-e1000-1/6-vrid-1)# owner
device(conf-if-e1000-1/6-vrid-1)# ipv6-address auto-gen-link-local
device(conf-if-e1000-1/6-vrid-1)# ipv6-address fd2b::1
device(conf-if-e1000-1/6-vrid-1)# activate
```

The following example configures a virtual IPv6 address for VRID 2 when VRRP-Ev3 is implemented. In this example, the device is configured as a VRRP-Ev3 backup device and the highest priority device will become the master VRRP-Ev3 device.

```
device# configure terminal
device(config)# ipv6 router vrrp-extended
device(config-ipv6-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 address fd4b::1/64
device(config-if-e1000-1/5)# ipv6 vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 110
device(config-if-e1000-1/5-vrid-2)# ipv6-address fe80::768e:f8ff:fe3a:0099
device(config-if-e1000-1/5-vrid-2)# ipv6-address fd4b::99
device(config-if-e1000-1/5-vrid-2)# activate
```

History

Release version	Command history
5.9.00	This command was modified to add the **auto-gen-link-local** keyword that auto-generates an IPv6 virtual link-local address.

ipv6 dhcp-relay include-options

Includes the parameters on the IPv6 DHCP relay agent messages.

Syntax

ipv6 dhcp-relay include-options [**interface-id**] [**remote-id**] [**client-mac-address**]

no ipv6 dhcp-relay include-options [**interface-id**] [**remote-id**] [**client-mac-address**]

Command Default

The parameters are not included on the IPv6 DHCP relay agent messages.

Parameters

interface-id

Includes the interface-ID parameter (option 18) in the IPv6 DHCP relay agent messages.

remote-id

Includes the remote-ID (option 37) parameter in the IPv6 DHCP relay agent messages.

client-mac-address

Includes the client link layer address (option 79) in the relay-forward messages.

Modes

Interface configuration mode

Usage Guidelines

The interface-ID parameter on the DHCPv6 relay forward message is used to identify the interface on which the client message is received. By default, this parameter is included only when the client message is received with the link-local source address.

You can enter either one or all of the include options as identifiers to specify in the relay-forward message.

The **no** form of the command disables the relay agent include options parameters.

Examples

The following example includes the **client-mac-address** parameter on the DHCPv6 relay agent messages.

```
device(config)# interface ethernet 1/3
device(config-if-eth-1/3)# ipv6 dhcp-relay include-options client-mac-address
```

History

Release version	Command history
5.4	This command was introduced.

Release version	Command history
5.9	This command was modified.

ipv6 match-payload-len

The IPv6 payload length range can be updated on all PPCR of a slot or one PPCR of slot or all PPCR of all slots. The Min and Max value of payload length range are included in comparison.

Syntax

ipv6 match-payload-len slot{ **all** | **slot** *number* } [**ppcr** *ppcr_id*] [**range** *Min Max*]

ipv6 match-payload-len

Command Default

No IPv6 payload length based filtering using ACL is applied to the interface.

Parameters

slot

Slot number.

all

All slots.

range

Payload length range.

min

Minimum of the payload length range.

max

Maximum of the payload length range.

Modes

Interface subtype configuration modes.

Usage Guidelines

To remove IP payload length based filtering using ACL, use the **no** form of this command.

Examples

Configure IPv6 payload length across system

```
device(config)#ipv6 match-payload-len slot all range 700 1000
```

Configure IPv6 payload length on all PPCR on given slot

```
device(config)#ipv6 match-payload-len slot 2 range 800 800
```

Configure IPv6 payload length on selected PPCR

```
device(config)#ipv6 match-payload-len slot 1 ppcr 1 range 0 1000
```

Removing IPv6 payload length configuration from selected PPCR

```
device(config)#no ipv6 match-payload-len slot 2 ppcr 1
```

History

Release version	Command history
6.0.00a	This command was introduced.

ipv6 mroute

Configures a multicast IPv6 static route for an interface.

Syntax

ipv6 mroute *dest-ipv6-prefix*/*prefix-length* [**ve** *ve-id* | **ipv6_tnl** *tunnel-id* | **6to4_tnl** *tunnel_id*] [*next-hop-ipv6-address*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

ipv6 mroute *dest-ipv6-prefix*/*prefix-length* [**ethernet** *slot/port* [*next-hop-ipv6-address*]] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

ipv6 mroute *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

ipv6 mroute *dest-ipv6-prefix*/*prefix-length* **null0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 mroute *dest-ipv6-prefix*/*prefix-length* [**ve** *ve-id* | **ipv6_tnl** *tunnel-id* | **6to4_tnl** *tunnel_id*] [*next-hop-ipv6-address*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

no ipv6 mroute *dest-ipv6-prefix*/*prefix-length* [**ethernet** *slot/port* [*next-hop-ipv6-address*]] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

no ipv6 mroute *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 mroute *dest-ipv6-prefix*/*prefix-length* **null0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

Command Default

An IPv6 static route is not configured.

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 prefix.

next-hop-ipv6-address
IPv6 address of the next-hop gateway.

next-hop-vrf *vrf_namenext-hop-ipv6-address*
Specifies a VRF instance and a next-hop IPv6 address.

null0
Causes packets to the selected destination to be dropped by shunting them to the "null0" interface. (This is the only available option.)

ethernet *slot/port*
Specifies the Ethernet slot or port.

ve *ve-id*
Specifies the virtual Ethernet (VE) interface VE ID.

6to4_tnl *tunnel-id*

Specifies IPv6 to IPv4 tunnel number to be used as next hop.

ipv6_tnl *tunnel-id*

Specifies IPv6 tunnel to be used as next hop.

name *string*

Optional name (ASCII string) assigned to the route.

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 255. 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.

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 IPv6 static route redistribution).

tag-number

A number from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command removes the multicast static route. If the route is named, the **no** form of the command must be used twice, the first time to remove the name and the second time to remove the route.

The **ethernet** *slot/port* designation for the destination does not apply to PIM SM.

Examples

The following example configures an IPv6 static route by specifying the destination prefix and the outgoing interface.

```
device# configure terminal
device(config)#vrf green
device(config-vrf-green)#address-family ipv6
device(config-vrf-green-ipv6)#ipv6 mroute 2002::/64 eth 1/1
```

The static route can also be configured with outgoing interface as **ve**, such as **ve 10** as shown in the following example.

```
device# configure terminal
device(config)#vrf green
device(config-vrf-green)#address-family ipv6
device(config-vrf-green-ipv6)#ipv6 mroute 2003::/64 ve 10
```

ipv6 mroute next-hop-enable-default

You can enable an IPv6 default multicast static route to resolve other static routes.

Syntax

ipv6 mroute [**next-hop-enable-default**]

no ipv6 mroute [**next-hop-enable-default**]

Command Default

By default, the IPv6 default multicast static route is not used to resolve IPv6 multicast static route next hops.

Modes

Global configuration mode

Usage Guidelines

Before configuring an static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the **ipv6 unicast-routing** command and must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The **no** form of the command disables IPv6 multicast static route next-hop resolution through the default static route.

Examples

The following example enables the default multicast static route to resolve other static routes.

```
device# configure terminal
device(config)# ipv6 mroute next-hop-enable-default
```

ipv6 mroute next-hop-recursion

You can resolve multicast static route destinations using recursive lookup.

Syntax

ipv6 mroute [**next-hop-recursion** [*number*]

no ipv6 mroute [**next-hop-recursion** [*number*]

Command Default

By default, static route recursive lookup is not used to resolve IPv6 multicast static routes.

Parameters

number

Specifies the level of recursion for address lookup. The range is 1 through 10. If no number is specified, the default value is 3.

Modes

Global configuration mode

Usage Guidelines

Before configuring an IPV6 multicast static oute, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the **ipv6 unicast-routing** command, and you must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The **no** form of the command disables IPv6 multicast static route next-hop recursion.

Examples

The following example configures recursive static route lookup to five levels to resolve IPv6 multicast static routes.

```
device# configure terminal
device(config)# ipv6 mroute next-hop-recursion 5
```

ipv6 multicast-routing load-sharing rebalance

Enables or disables the rebalance of the load-sharing among ECMP IPv6 paths.

Syntax

ipv6 multicast-routing load-sharing [**rebalance**]

no ipv6 multicast-routing load-sharing [**rebalance**]

Parameters

rebalance

Specifies that the ECMP load-sharing will be rebalanced for the interface on which the **rebalance** keyword is configured.

Modes

Interface configuration mode

Examples

To configure IPv6 Multicast ECMP, use this command in the configuration mode.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ipv6 multicast-routing load-sharing
```

To disable load distribution among ECMP IP paths use the **no** form of the command.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# no ipv6 multicast-routing load-sharing
```

The following example configures rebalancing of the load distribution among ECMP IP paths.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ipv6 multicast-routing load-sharing rebalance
```

History

Release	Command History
5.5.00	This command was added to enable of disable the rebalance of the load-sharing among ECMP paths.

ipv6 multicast-routing optimization mct-scaling

Enables IPv6 PIM over MCT scaling optimization.

Syntax

ipv6 multicast-routing optimization mct-scaling

no ipv6 multicast-routing optimization mct-scaling

Command Default

PIM over MCT has a scaling limit of 2K mcache (S,G) entries and 512 MLD entries.

Modes

Global configuration mode.

Usage Guidelines

When you enable PIM over MCT scaling optimization, the maximum scaling of mcache entries to 16K entries and MLD entries to 4K entries.

The **no** form of the command resets the default scaling limits.

Examples

The following example configures MCT scaling optimization.

```
device# configure terminal
device(config)# ipv6 multicast-routing optimization mct-scaling
```

History

Release version	Command history
06.1.00	This command was introduced.

ipv6 nd proxy

Configures a single IPv6 subnet prefix to support multiple physical links in IPv6 Neighbor Discovery.

Syntax

ipv6 nd proxy

no ipv6 nd proxy

Command Default

This feature is disabled.

Modes

The `ipv6 nd proxy` is configurable under the global configuration mode.

Usage Guidelines

The IPv6 ND proxy command turns on the IPv6 ND proxy capability for the node, and is run at the configuration level.

Use the **no** form of this command to remove the ND proxy configuration.

Per RFC 4389, ND proxy can be used to bridge multiple links into a single entity to simplify management, as there is no need to allocate subnet numbers to the different networks. This can help alleviate the need to configure NAT in IPv6 networks.

> NOTE
> This is an IETF Experimental Protocol. It is the responsibility of the user to ensure that appropriate network-layer support is provided.

The following limitations apply:

The `ipv6 nd proxy` is not supported over v6 tunnel interface.

The `IPv6 nd proxy` programs the RACL to force the Unicast NS, sent during neighbor refresh, to the CPU for processing as proxy NS.

The `ipv6 nd proxy` is currently supported for NS and NA messages and are not supported for other ND messages like RS, RA and redirect message.

The `IPv6 nd proxy` is not supported for the IPsec tunnels and on MCT.

Examples

To enable the `IPv6 ND proxy` feature for the node:

```
R2>#en
No password has been assigned yet...
R2#conf t
R2(config)# ipv6 nd proxy
R2(config)#
```

ipv6 nd ra-dns-server

Advertises the recursive Domain Name System (DNS) server address and the lifetime multiplier information to IPv6 hosts in the Router Advertisement (RA) message.

Syntax

ipv6 nd ra-dns-server *ipv6-address* [**lifetime-multiplier** *decimal*]

no ipv6 nd ra-dns-server *ipv6-address* [**lifetime-multiplier** *decimal*]

Command Default

By default, the recursive DNS server address and the lifetime multiplier information is not configured.

Parameters

ipv6-address

Specifies the global IPv6 address of the DNS server.

lifetime-multiplier *decimal*

Specifies the percentage value of tthe maximun router advertisement interval. the maximum router advertisement interval is the maximum time that can be allowed between sending unsolicited RA messages for DNS name resolution. The lifetime-multiplier decimal value is calculated as a percentage of the RA lifetime. The maximum router advertisement interval percentage range is 100 percent through 200 percent and the default value is 200 percent.

Modes

Global configuration mode.

Interface configuration mode.

Usage Guidelines

You can configure a maximum of four recursive DNS server addresses and corresponding lifetime multiplier values at a given instance.

no

NOTE

The **ipv6 nd ra-dns-server** command at the interface configuration level takes precedence over global configuration. In other words, if at least one DNS server address is configured on an interface, it will override other DNS server address configurations at the global configuration.

Examples

The following examples configure the recursive DNS address for a lifetime-multiplier value of 200.

```
device(config)# ipv6 nd ra-dns-server 2001:DC8:200::3 lifetime 200
device(config-if-e10000-1/10)# ipv6 nd ra-dns-server 2001:DC8:200::3 lifetime 200
```

ipv6 nd ra-domain-name

Configures the domain name of the Domain Name System (DNS) suffix and the lifetime multiplier information to IPv6 hosts in the Router Advertisement (RA) message. The **no** form of this command disables the advertisement of the specified domain name of DNS suffix in the RA message.

Syntax

ipv6 nd ra-domain-name *string* [**lifetime-multiplier** *decimal*]

no ipv6 nd ra-domain-name *string* [**lifetime-multiplier** *decimal*]

Parameters

string	Specifies the domain name of the DNS suffix.
lifetime-multiplier ***decimal***	Specifies the percentage value of maximum router advertisement interval. The maximum router advertisement interval is the maximum time that can be allowed between sending unsolicited RA messages for DNS name resolution. The **lifetime-multiplier** *decimal* **value is calculated as percentage of** the RA lifetime. **The maximum router advertisement interval percentage range is 100 through 200% and the default value is 200%.**

Modes

Global configuration mode.

Interface configuration mode.

Usage Guidelines

You can configure a maximum of four different domain names of DNS suffix and corresponding lifetime multiplier values at a given instance.

The domain name of a DNS suffix at the global configuration level is used on all IPv6 routed interfaces that do not have a domain name of DNS suffix configured on them.

NOTE

The **ipv6 nd ra-domain-name** command at the interface configuration takes precedence over global configuration. In other words, if at least one DNS server address is configured on an interface, it will override other DNS server address configurations at the global configuration.

Examples

The following examples configure the domain names of a DNS suffix for a lifetime-multiplier value of 200.

```
device (config)# ipv6 nd ra-domain-name brocade.com lifetime 200
device (config-if-e10000-1/10)# ipv6 nd ra-domain-name brocade.com lifetime 200
```

History

Release	Command History
5.5.00	This command was introduced.

ipv6 ospf active

Sets a specific OSPFv3 interface to active.

Syntax

ipv6 ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ipv6 ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPFv3 control packets.

Examples

The following example sets a specific OSPFv3 Ethernet interface to active.

```
device# configure termnial
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf active
```

ipv6 ospf area

Enables OSPFv3 on an interface.

Syntax

ipv6 ospf area *area-id* | *ip-addr*

no ipv6 ospf area

Command Default

OSPFv3 is disabled.

Parameters

area-id

Area ID in dotted decimal or decimal format.

ip-addr

Area ID in IP address format.

Modes

Interface subtype configuration mode

Usage Guidelines

This command enables an OSPFv3 area on the interface to which you are connected.

The **no** form of the command disables OSPFv3 on this interface.

Examples

The following example enables a configured OSPFv3 area named 0 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
```

ipv6 ospf authentication ipsec

Specifies IP security (IPsec) as the authentication type for an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec key-add-remove-interval *interval*

no ipv6 ospf authentication ipsec key-add-remove-interval *interval*

Command Default

Disabled.

Parameters

key-add-remove-interval *interval*

Specifies the OSPFv3 authentication key add-remove interval. Valid values range from decimal numbers 0 through 14400. The default is 300.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command removes IPsec authentication from the interface.

Examples

The following example enables IPsec on a specified OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec
```

The following example sets the OSPFv3 authentication key add-remove interval to 480.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec key-add-remove-interval 480
```

ipv6 ospf authentication ipsec disable

Disables IP security (IPsec) services on an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec disable

no ipv6 ospf authentication ipsec disable

Command Default

Authentication is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to disable IPsec if it is enabled on the interface. Packets that are sent out will not be IPSec encapsulated and the received packets which are IPSec encapsulated will be dropped.

The **no** form of the command re-enables IPSec on the interface if IPsec is already configured on the interface.

Examples

The following example disables IPsec on a specific OSPFv3 interface where IPsec is already enabled.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec disable
```

ipv6 ospf authentication ipsec spi

Specifies the IP security (IPsec) security policy index (SPI) value for an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec spi *value* **esp sha1** *key* [**no-encrypt**] *key* }

no ipv6 ospf authentication spi

Command Default

Authentication is disabled.

The 40-hexadecimal character key is encrypted by default. Use the **no-encrypt** parameter to disable encryption.

Parameters

ipsec

Specifies IPsec as the authentication protocol.

spi

Specifies the Security Policy Index (SPI).

value

Specifies the SPI value. Valid values range from decimal numbers 256 through 4294967295. The near-end and far-end values must be the same.

esp

Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security. This is the only option currently available.

sha1

Enables Hashed Message Authentication Code (HMAC) Secure Hash Algorithm 1 (SHA-1) authentication.

key

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

no-encrypt

The 40-character key is not encrypted upon either its entry or its display.

key

The 40 hexadecimal character key.

Modes

Interface subtype configuration mode

Usage Guidelines

The 40 hexadecimal character key is encrypted by default. The system adds the following in the configuration to indicate that the key is encrypted:

- encrypt = the key string uses proprietary simple cryptographic 2-way algorithm (only for Brocade NetIron CES and Brocade NetIron CER devices)
- encryptb64 = the key string uses proprietary base64 cryptographic 2-way algorithm (only for Brocade NetIron XMR and Brocade MLX series devices)

To change an existing key, you must specify a different SPI value to that of the value already configured.

The **no** form of the command removes 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 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec spi 512 esp sha1
abcef12345678901234fedcba098765432109876
```

ipv6 ospf bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv3 interface.

Syntax

ipv6 ospf bfd disable

no ipv6 ospf bfd

Command Default

BFD is disabled by default.

Parameters

disable

Disables BFD on the OSPFv3 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated if BFD is also enabled globally using the **bfd all-interfaces** command in OSPFv3 router configuration mode. If BFD is disabled using the **no bfd all-interfaces** 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 a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf bfd
```

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

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf bfd disable
```

ipv6 ospf cost

Configures cost for a specific OSPFv3 interface.

Syntax

ipv6 ospf cost *value*

no ipv6 ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv3 cost on the interface. If the cost is not configured with this command, OSPFv3 calculates the value from the reference and interface bandwidths.

For more information, refer to the **auto-cost reference-bandwidth** command.

The **no** form of the command disables the configured cost.

Examples

The following example sets the cost to 620 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf cost 620
```

ipv6 ospf dead-interval

Specifies the time period for which a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ipv6 ospf dead-interval *interval*

no ipv6 ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 65535 seconds. The default is 40.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the **ipv6 ospf hello-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.
- The default OSPF timer values of 10 seconds for the hello-interval and 40 seconds for the dead-interval or higher are recommended on Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

The **running-config** command displays only explicitly configured values of the hello interval, which means that a value that was automatically changed as the result of a dead-interval change is not displayed.

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

Examples

The following example sets the dead interval to 80 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf dead-interval 80
```

ipv6 ospf hello-interval

Sets the length of time between the transmission of hello packets that an interface sends to neighbor routers.

Syntax

ipv6 ospf hello-interval *interval*

no ipv6 ospf hello-interval

Command Default

The length of time between the transmission of hello packets is set to 10 seconds.

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535 seconds. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello interval, unless the dead interval is also explicitly configured using the **ipv6 ospf dead-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.
- The default OSPF timer values of 10 seconds for the hello-interval and 40 seconds for the dead-interval or higher are recommended on Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello interval change is not displayed.

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

Examples

The following example sets the hello interval to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf hello-interval 20
```

ipv6 ospf hello-jitter

Sets the allowed jitter between HELLO packets.

Syntax

ipv6 ospf hello-jitter *interval*

no ipv6 ospf hello-jitter

Parameters

jitter

Allowed interval between hello packets.Valid values range from 1 through 50 percent (%).

Modes

Interface subtype configuration mode

Usage Guidelines

The hello interval can vary from the configured hello-interval to a maximum of percentage value of configured jitter.

Examples

The following example sets the hello jitter to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf hello-jitter 20
```

ipv6 ospf instance

Specifies the number of OSPFv3 instances running on an interface.

Syntax

ipv6 ospf instance *instanceID*

no ipv6 ospf instance

Parameters

instanceID

Instance identification number. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

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

Examples

The following example sets the number of IPv6 OSPF instances to 35 on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf instance 35
```

ipv6 ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Command Default

Enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv3 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The **no** no form of the command disables MTU-match checking on a specific interface.

Examples

The following example disables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# no ipv6 ospf mtu-ignore
```

The following example enables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf mtu-ignore
```

ipv6 ospf network

Configures network type.

Syntax

ipv6 ospf network { **broadcast** | **point-to-point** }

no ipv6 ospf network

Command Default

Network type is broadcast for Ethernet and VE interfaces. Network type is point-to-point for tunnel and GRE interfaces.

Parameters

broadcast

Network type is broadcast, such as Ethernet.

point-to-point

Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

Point-to-point can support unnumbered links, which requires less processing by OSPFv3.

The **no** form of the command removes the network-type configuration.

NOTE

The network type non-broadcast is not supported at this time.

Examples

The following example configures an OSPFv3 point-to-point link on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf network point-to-point
```

The following example configures an OSPFv3 broadcast link on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf network broadcast
```

ipv6 ospf passive

Sets a specific OSPFv3 interface to passive.

Syntax

ipv6 ospf passive

no ipv6 ospf passive

Modes

Interface subtype configuration mode

Usage Guidelines

The **ipv6 ospf passive** command disables transmission of OSPFv3 control packets on that interface. OSPFv3 control packets received on a passive interface are discarded.

The **no** form of the command sets an interface back to active.

Examples

The following example sets a specific OSPFv3 Ethernet interface to passive.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf passive
```

ipv6 ospf priority

Configures priority for designated router (DR) election and backup designated routers (BDRs) on the interface you are connected to.

Syntax

ipv6 ospf priority *value*

no ipv6 ospf priority

Command Default

The value is set to 1.

Parameters

value

Priority value. Valid values range from 0 through 255. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv3 router assigned the highest priority becomes the designated router, and the OSPFv3 router with the second-highest priority becomes the backup router.

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

Examples

The following example sets a priority of 4 for the OSPFv3 router that is connected to an OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf priority 4
```

ipv6 ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

Syntax

ipv6 ospf retransmit-interval *interval*

no ipv6 ospf retransmit-interval

Command Default

The interval is 5 seconds.

Parameters

interval

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds. The default is 5.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

Examples

The following example sets the retransmit interval to 8 for all OSPFv3 devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf retransmit-interval 8
```

ipv6 ospf suppress-linklsa

Suppresses link LSA advertisements.

Syntax

ipv6 ospf suppress-linklsa

no ipv6 ospf suppress-linklsa

Modes

Interface subtype configuration mode

Examples

The following example suppresses link LSAs from being advertised on devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf suppress-linklsa
```

ipv6 ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv3 to send link-state update packets on the interface to which you are connected.

Syntax

ipv6 ospf transmit-delay *value*

no ipv6 ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

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

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf transmit-delay 25
```

ipv6 rate-limit hoplimit-expired-to-cpu

Applies rate-limit option on IPv6 hop-limit packets, if the hop-limit count is less than or equal to one.

Syntax

ipv6 rate-limit hoplimit-expired-to-cpu *rate-limit policy*

no ipv6 rate-limit hoplimit-expired-to-cpu *rate-limit policy*

Command Default

By default, the no rate-limit option is applied to IPv6 hop-limit packets, if the hop-limit count is less than or equal to one.

Parameters

rate-limit policy

Name of the policy-map.

Modes

Global configuration mode,

Usage Guidelines

Create CPU bound rate-limit policy map before applying rate-limiting for hop-limit packets.

NOTE

The following warning message is displayed if only some of the cards are supported and few are not supported.

```
Warning: rate-limit config for protocol "hoplimit-expired-to-cpu" is not supported on module 1, 3
```

NOTE

The following warning message is displayed if none of the cards are supported.

```
Warning: rate-limit config for protocol "hoplimit-expired-to-cpu" is not supported on available
modules.
It is only supported on GEN-2 and later modules.
```

The **no** form of the command disables rate-limit option on IPv6 hop-limit packets.

Examples

The following example explains how to apply a rate-limit policy for IPv6 hop-limit packets.

```
device(config)# ipv6 rate-limit hoplimit-expired-to-cpu policy-map save-cpu-policy
```

History

Release version	Command history
5.8.00	This command was introduced.

ipv6 receive access-list

Configures an IPv6 access-control list as an IPv6 receive access-control list (rACL).

Syntax

ipv6 receive access-list *acl-name* **sequence** *seq-num* [**policy-map** *policy-map-name* [**strict-acl**]]

no ipv6 receive access-list *acl-name* **sequence** *seq-num* [**policy-map** *policy-map-name* [**strict-acl**]]

Parameters

acl-name	Specifies the name of the access-control list to apply to all interfaces within the default VRF, for all CPU-bound traffic. The maximum length of the access-control list name is 256 characters.
sequence *seq-num*	Defines the sequence number of the access-control list being applied as a rACL. IPv6 rACL commands are applied in the order of the lowest to the highest sequence numbers. The range of values is from 1 through 50.
policy-map *policy-map-name*	Specifies the name of a policy map. When the **policy-map** option is specified, traffic matching the "permit "clause of the specified IPv6 ACL is rate-limited as defined in the policy map and IPv6 traffic matching the "deny" clause in the IPv6 ACL is permitted without any rate limiting.
strict-acl	Specifies that traffic matching the "permit" clause of the specified IPv6 ACL is rate-limited as defined in the policy map and IPv6 traffic matching the "deny" clause in the IPv6 ACL is dropped in the hardware.

Modes

Global configuration mode

Usage Guidelines

The rACL works like a regular ACL where IPv6 traffic matching the "permit" clause specified in the IPv6 ACL is permitted, and IPv6 traffic matching the "deny" clause in the IPv6 ACL is dropped in hardware.

The **no** form of the basic command removes the rACL.

The **no** form of the command with both **policy-map** and **strict-acl** options specified, removes the **strict-acl** option: the rACL with **policy-map** remains and traffic matching "deny" clauses starts passing to the CPU.

Examples

The following example configures an IPv6 rACL to apply the ACL "b1" with a sequence number of "15" to all interfaces within the default VRF, for all CPU-bound traffic.

```
device(config)# ipv6 receive access-list b1 sequence 15
```

The following example configures an IPv6 rACL with a policy map "m1". The rACL applies the ACL "b1" with a sequence number of "15" to all interfaces within the default VRF, for all CPU-bound traffic. Traffic matching the permit clause of the "b1" ACL is rate-limited as defined in in the policy map "m1" and traffic matching the "deny" clause in "b1" ACL is permitted without any rate limiting.

```
device(config)# ipv6 receive access-list b1 sequence 15 policy map m1
```

The following example removes the **strict-acl** option so that traffic matching "deny" clauses starts passing to the CPU: the rACL with the policy map "m1" remains.

```
device(config)# no ipv6 receive access-list b1 sequence 15 policy-map m1 strict-acl
```

History

Release version	Command history
5.6.00	This command was modified to support named rACLs.

ipv6 receive access-list enable-deny-logging

Generates logs for a specific interface that contain IPv6 packets that are denied as a result of a receive access-control list (rACL).

Syntax

ipv6 receive access-list enable-deny-logging [**hw-drop**]

no ipv6 receive access-list enable-deny-logging [**hw-drop**]

Command Default

Logs are not generated for IPv6 packets that are denied by an rACL.

Parameters

hw-drop

Drops the denied IPv6 packets in hardware.

Modes

Interface configuration mode

Usage Guidelines

By default, any IPv6 packets received on an interface that are denied by an rACL are discarded by the software. To avoid high CPU usage when you enable the log generation of denied IPv6 packets, configure the optional **hw-drop** keyword to drop the IPv6 packets in the hardware after the log is generated.

The **no** form of this command disables the log generation.

NOTE
The **ipv6 receive access-list enable-deny-logging** command is supported only on Brocade NetIron MLX Series devices.

Examples

The following example creates an rACL to deny packets and enables the generation of IPv6 packet logging on Ethernet interface 1/1.

```
device# configure terminal
device(config)# ipv6 receive access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 receive access-list deny-log in
device(config-if-e1000-1/1)# ipv6 receive access-list enable-deny-logging
```

The following example creates an rACL to deny packets, enables the generation of IPv6 packet logging on Ethernet interface 1/1 and drops the packets in hardware.

```
device# configure terminal
device(config)# ipv6 receive access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 receive access-list deny-log in
device(config-if-e1000-1/1)# ipv6 receive access-list enable-deny-logging hw-drop
```

History

Release version	Command history
5.9.00a	This command was introduced.

ipv6 receive access-list enable-permit-logging

Generates logs of IPv6 packets permitted by receive access-control lists (rACLs) applied at device level.

Syntax

ipv6 receive access-list enable-permit-logging [**selective**]

no ipv6 receive access-list enable-permit-logging [**selective**]

Command Default

Logs are not generated for IPv6 packets that are permitted by an rACL.

Parameters

selective

Configures logging of permitted traffic to include only the first packet in each time cycle.

Modes

Global configuration mode

Usage Guidelines

IPv6 ACL logging is not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.

To avoid high CPU usage under permit log generation, include the **selective** keyword.

The **no** form of this command disables the log generation.

Examples

The following example enables IPv6 rACL permit logging on the device.

```
device# configure terminal
device(config)# ipv6 receive access-list enable-permit-logging
```

The following example sets the **ipv6 session-logging-age** parameter to 7 minutes and—for IPv6 rACLs—configures permit logging on the device as selective.

```
device# configure terminal
device(config)# ipv6 session-logging-age 7
device(config)# ipv6 receive access-list enable-permit-logging selective
```

History

Release version	Command history
6.0.00a	This command was introduced.

ipv6 receive deactivate-acl-all

Deactivates the IPv6 receive access-control list (rACL) configuration and removes all rules from Content Addressable Memory (CAM). The **no** form of this command re-activates the rACL configuration.

Syntax

ipv6 receive deactivate-acl-all

no ipv6 receive deactivate-acl-all

Modes

Global configuration mode.

Usage Guidelines

Use the **write memory** command to save this configuration permanently and to prevent ACL binding to CAM after reload.

The **no** version of the command removes the configured deactivate option and sets it to default.

Examples

The following example deactivates the IPv6 rACL configuration.

```
device(config)# ipv6 receive deactivate-acl-all
```

The following example re-activates the IPv6 rACL configuration.

```
device(config)# no ipv6 receive deactivate-acl-all
```

History

Release	Command History
5.6.00	This command was introduced.

ipv6 receive delete-acl-all

Deletes IPv6 receive access-control list (rACL) rules from the system.

Syntax

ipv6 receive delete-acl-all

Modes

Global configuration mode.

Usage Guidelines

You must confirm that you wish to proceed with the deletion. Enter 'y' or 'n' in response to the prompt "Are you sure?.

Examples

The following example deletes all IPv6 rACL rules from the system.

```
device(config)# ipv6 receive delete-acl-all
This command deletes all IP Receive ACLs from system.
Are you sure? (enter 'y' or 'n'):y
```

History

Release	Command History
5.6.00	This command was introduced.

ipv6 receive rebind-acl-all

Rebinds an IPv6 receive access-control list (rACL).

Syntax

ipv6 receive rebind-acl-all

Modes

Global configuration mode.

Usage Guidelines

When access list rules are modified or a policy map associated with a rACL is changed, an explicit rebind must be performed to propagate the changes to the interfaces.

Examples

The following example rebinds an IPv6 rACL.

```
device(config)# ipv6 receive rebind-acl-all
```

History

Release	Command History
5.6.00	This command was introduced.

ipv6 route

Configures a static IPv6 route for an interface.

Syntax

ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ve** *ve-id* | **ipv6_tnl** *tunnel-id* | **6to4_tnl** *tunnel_id*] [*link-local-next-hop-ipv6-address*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ethernet** *slot/port* [*link-local-next-hop-ipv6-address*]] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

ipv6 route *dest-ipv6-prefix*/*prefix-length* **null0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ve** *ve-id* | **ipv6_tnl** *tunnel-id* | **6to4_tnl** *tunnel_id*] [*link-local-next-hop-ipv6-address*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* [**ethernet** *slot/port* [*link-local-next-hop-ipv6-address*]] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *string*]

no ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* **null0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

Command Default

An IPv6 static route is not configured.

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 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.

next-hop-vrf *vrf_name next-hop-ipv6-address*
: Specifies a VRF instance and a next-hop IPv6 address.

null0
: Causes packets to the selected destination to be dropped by shunting them to the "null0" interface. (This is the only available option.)

ethernet *slot/port*
: Specifies the Ethernet slot or port.

ve *ve-id*

Specifies the virtual Ethernet (VE) interface VE ID.

6to4_tnl *tunnel-id*

Specifies IPv6 to IPv4 tunnel number to be used as next hop.

ipv6_tnl *tunnel-id*

Specifies IPv6 tunnel to be used as next hop.

name *string*

Optional name (ASCII string) assigned to the route

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 255. 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.

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

The **no** form of the command removes the IPv6 static route. If the route is named, the **no** command must be used twice, the first time to remove the name and the second time to remove the route.

Examples

To configure the IPv6 ND proxy static route by specifying the destination prefix and the outgoing interface:

> NOTE
> As per the topology mentioned in the packet flow, if the IPv6 ND proxy is configured on R2, then this static route can be configured on R1 with the destination prefix being 2002::/64. The static route can also be configured with outgoing interface as **ve**, such as **ve 10**.

```
R1(config)#
R1(config)# ipv6 route 2002::/64 ethernet 1/1

R1(config)#
R1(config)# ipv6 route 2003::/64 ve 10

R1(config)# vrf green
R1(config-vrf-green)# address-family ipv6
R1(config-vrf-green-ipv6)# ipv6 route 2002::/64 eth 1/1

R1(config)#vrf green
R1(config-vrf-green)# address-family ipv6
R1(config-vrf-green-ipv6)# ipv6 route 2003::/64 ve 10
```

To **show** the **running-config** (with truncated output showing only the static route):

```
R1(config)# ipv6 route 2002::/64 ethernet 1/1
R1(config)# ipv6 route 2003::/64 ve 10

vrf green
 rd 66:66
 address-family ipv6
 ipv6 route 2002::/64 ethernet 1/1
 ipv6 route 2003::/64 ve 10
R1(config)#exit-vrf
```

ipv6 route bfd

Enables Bidirectional Forwarding Detection (BFD) monitoring for an IPv6 static route.

Syntax

ipv6 route *dest-ipv6-prefix/prefix-length next-hop-ipv6-address* **bfd**

ipv6 route *dest-ipv6-prefix/prefix-length next-hop-ipv6-address* **bfd** [*metric* | **distance** *number* | **name** *name* | **tag** *number*]

Command Default

BFD monitoring for an IPv6 static route is not enabled.

Parameters

dest-ipv6-prefix
Specifies the destination IPv6 prefix in hexadecimal with 16-bit values between colons.

prefix-length
A decimal value specifying the length of the IPv6 prefix.

next-hop-ipv6-address
Specifies the IPv6 address of the next hop.

metric
Specifies the cost metric of the route. Valid values range from 1 through 16. The default is 1.

distance *number*
Specifies the administrative distance of the route. Valid values range from 1 through 255. The default is 1.

name *name*
Specifies the name of the route in ASCII characters.

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

Usage Guidelines

The **no** form of the command removes BFD monitoring from the static route.

Examples

The following example enables BFD route monitoring on an IPv6 static route and sets the cost metric of the route to 10.

```
device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd 10
```

The following example enables BFD route monitoring on an IPv6 static route and sets the administrative distance of the route to 55.

```
device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd distance 55
```

The following example enables BFD route monitoring on an IPv6 static route and sets the name of the route to “routered”.

```
device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd name routered
```

The following example enables BFD route monitoring on an IPv6 static route and sets the tag value of the route to 100.

```
device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd tag 100
```

ipv6 route next-hop

Enables the Brocade device to use routes from a specified protocol to resolve a configured IPv6 static route.

Syntax

ipv6 route next-hop { **bgp** | **isis** | **ospf** | **rip** }

no ipv6 route next-hop { **bgp** | **isis** | **ospf** | **rip** }

Command Default

The Brocade device is not enabled to use routes from a specified protocol to resolve a configured IPv6 static route.

Parameters

bgp

Configures the device to use iBGP and eBGP routes to resolve static routes.

isis

Configures the device to use ISIS to resolve static routes.

ospf

Configures the device to use OSPF routes to resolve static routes.

rip

Configures the device to use RIP routes to resolve static routes.

Modes

Global configuration mode

Usage Guidelines

Before configuring a static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the **ipv6 unicast-routing** command and enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The **no** form of the command disables IPv6 static route resolution through the designated protocol.

Examples

The following example configures the device to use OSPF protocol to resolve IPv6 static routes.

```
device# configure terminal
device(config)# ipv6 route next-hop ospf
```

ipv6 route next-hop-enable-default

You can enable the IPv6 default static route to resolve other static routes.

Syntax

ipv6 route [**next-hop-enable-default**]

no ipv6 route [**next-hop-enable-default**]

Command Default

By default, the IPv6 default static route is not used to resolve IPv6 static route next hops.

Modes

Global configuration mode

Usage Guidelines

Before configuring a static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the **ipv6 unicast-routing** command and must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The **no** form of the command disables IPv6 static route next-hop resolution through the default static route.

Examples

The following example enables the default static route to resolve other static routes.

```
device# configure terminal
device(config)# ipv6 route next-hop-enable-default
```

ipv6 next-hop-recursion

You can resolve static route destinations using recursive lookup.

Syntax

ipv6 route [**next-hop-recursion** [*number*]

no ipv6 route [**next-hop-recursion** [*number*]

Command Default

By default, static route recursive lookup is not used to resolve IPv6 static routes.

Parameters

number

Specifies the level of recursion for address lookup. The range is 1 through 10. If no number is specified, the default value is 3.

Modes

Global configuration mode

Usage Guidelines

Before configuring a static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the **ipv6 unicast-routing** command, and you must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The **no** form of the command disables IPv6 static route next-hop recursion.

Examples

The following example configures recursive static route lookup to five levels to resolve IPv6 static routes.

```
device# configure terminal
device(config)# ipv6 route next-hop-recursion 5
```

ipv6 route static-bfd

Configures Bidirectional Forwarding Detection (BFD) session parameters for IPv6 static routes.

Syntax

ipv6 route [**vrf** *vrf-name*] **static-bfd** *dest-ipv6-address source-ipv6-address* [**interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

no ipv6 route [**vrf** *vrf-name*] **static-bfd** *dest-ipv6-address source-ipv6-address*

Command Default

BFD is not configured for an IPv6 static route.

Parameters

vrf *vrf-name*
Specifies the name of a VRF instance.

dest-ipv6-address
Specifies the destination IPv6 address.

source-ipv6-address
Specifies the source IPv6 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.

min-rx *receive-time*
Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000.

multiplier *number*
Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD determines that the connection to that peer is not operational. Valid values range from 3 through 50.

Modes

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 multi-hop BFD sessions, if the configured **interval** and **min-rx** parameters conflict with those of an existing BGP 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.

When Brocade NetIron CER Series or Brocade NetIron CES Series devices are heavily loaded or under stress, BFD sessions may flap if the configured BFD interval is less than 500 milliseconds with a multiplier value of 3.

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.

```
device# configure terminal
device(config)# ipv6 route static-bfd fe80::a fe80::b interval 100 min-rx 100 multiplier 10
```

ipv6 router ospf

Enables and configures the Open Shortest Path First version 3 (OSPFv3) routing protocol.

Syntax

ipv6 router ospf [**vrf** *name*]

no ipv6 router ospf

Command Default

Disabled.

Parameters

vrf *name*

Specifies a nondefault VRF.

Modes

Global configuration mode

Usage Guidelines

If you save the configuration to the startup-config file after disabling OSPFv3, all OSPFv3 configuration information is removed from the startup-config file.

Use this command to enable the OSPFv3 routing protocol and enter OSPFv3 router or OSPFv3 router VRFconfiguration mode. OSPFv3 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

The **no** form of the command deletes all current OSPFv3 configurations and blocks any further OSPFv3 configuration.

Examples

The following example enables OSPFv3 on a default VRF and enters OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)#
```

ipv6 router vrrp

Globally enables IPv6 Virtual Router Redundancy Protocol (VRRP).

Syntax

ipv6 router vrrp

no ipv6 router vrrp

Command Default

IPv6 VRRP is not globally enabled.

Modes

Global configuration mode

Usage Guidelines

After globally enabling IPv6 VRRP, the command prompt does not change. Nearly all subsequent IPv6 VRRP configuration is performed at the interface level, but IPv6 VRRP must be enabled globally before configuring IPv6 VRRP instances.

The **no** form of the command disables VRRP globally.

Examples

The following example enables IPv6 VRRP globally and enters interface configuration mode to allow you to enter more VRRP configuration.

```
device# configure terminal
device(config)# ipv6 router vrrp
device(config-ipv6-vrrp-router)# interface ethernet 1/4
device(config-if-e1000-1/4)# ipv6 address fd3b::3/64
device(config-if-e1000-1/4)# ipv6 vrrp vrid 2
device(config-if-e1000-1/4-vrid-2)# backup priority 100
device(config-if-e1000-1/4-vrid-2)# version 3
device(config-if-e1000-1/4-vrid-2)# advertise backup
device(config-if-e1000-1/4-vrid-2)# ipv6-address fe80::768e:f8ff:fe2a:0099
device(config-if-e1000-1/4-vrid-2)# ipv6-address fd3b::2
device(config-if-e1000-1/4-vrid-2)# activate
```

ipv6 router vrrp-extended

Globally enables IPv6 Virtual Router Redundancy Protocol Extended (VRRP-E).

Syntax

ipv6 router vrrp-extended

no ipv6 router vrrp-extended

Command Default

VRRP-E is not globally enabled.

Modes

Global configuration mode

Usage Guidelines

After globally enabling IPv6 VRRP-E, nearly all subsequent IPv6 VRRP-E configuration is performed at the interface level. If IPv6 VRRP-E is not globally enabled, you will see an error message when configuring IPv6 VRRP-E instances.

The **no** form of the command disables VRRP-E globally.

Examples

The following example enables IPv6 VRRP-E globally and enters interface configuration mode for subsequent IPv6 VRRP-E configuration.

```
device# configure terminal
device(config)# ipv6 router vrrp-extended
device(config-ipv6-vrrpe-router)# interface ethernet 1/5
```

ipv6 traffic-filter

Applies an IPv6 ACL to incoming or outgoing traffic on an interface.

Syntax

ipv6 traffic-filter *acl-name* { **in** | **out** }

no ipv6 traffic-filter *acl-name* { **in** | **out** }

Command Default

No IPv6 ACL is applied to the interface.

Parameters

acl-name

Specifies the name of the IPv6 ACL.

in

Applies the ACL to incoming IPv6 packets on the interface.

out

Applies the ACL to outgoing IPv6 packets on the interface.

Modes

Interface subtype configuration modes

Usage Guidelines

To remove an ACL from an interface, use the **no** form of this command.

Examples

The following example creates an IPv6 ACL, defines within it a rule that blocks all Telnet traffic received from IPv6 host 2000:2382:e0bb::2, and applies the ACL to port 1/1.

```
device# configure terminal
device(config)# ipv6 access-list fdry
device(config-ipv6-access-list-fdry)# deny tcp host 2000:2382:e0bb::2 any eq telnet
device(config-ipv6-access-list-fdry)# permit ipv6 any any
device(config-ipv6-access-list-fdry)# exit
device(config)# interface ethernet 1/1
device(config-if-1/1)# ipv6 traffic-filter fdry in
device(config-if-1/1)# exit
device(config)# write memory
```

The first phase of the following example creates an IPv6 ACL, and defines the following rules within:

- Permit ICMP traffic from hosts in the 2000:2383:e0bb::x network to hosts in the 2001:3782::x network.
- Deny all IPv6 traffic from host 2000:2383:e0ac::2 to host 2000:2383:e0aa:0::24.
- Deny all UDP traffic.
- Permit all packets that are not explicitly denied by the other entries. (Without this entry, the ACL denies all incoming or outgoing IPv6 traffic on the ports to which the ACL is assigned.)

```
device# configure terminal
device(config)# ipv6 access-list netw
device(config-ipv6-access-list-netw)# permit icmp 2000:2383:e0bb::/64 2001:3782::/64
device(config-ipv6-access-list-netw)# deny ipv6 host 2000:2383:e0ac::2 host
2000:2383:e0aa:0::24
device(config-ipv6-access-list-netw)# deny udp any any
device(config-ipv6-access-list-netw)# permit ipv6 any any
device(config-ipv6-access-list-netw)# exit
```

The second phase of the example applies the ACL to both incoming and outgoing traffic on port 1/2 and to incoming traffic on port 4/3.

```
device(config)# interface ethernet 1/2
device(config-if-1/2)# ipv6 traffic-filter netw in
device(config-if-1/2)# ipv6 traffic-filter netw out
device(config-if-1/2)# exit
device(config)# interface ethernet 4/3
device(config-if-4/3)# ipv6 traffic-filter netw in
device(config-if-4/3)# exit
device(config)# write memory
```

ipv6 traffic-filter enable-deny-logging

Generates logs for a specific interface that contain IPv6 packets that are denied as a result of an access-control list (ACL).

Syntax

ipv6 traffic-filter enable-deny-logging [**hw-drop**]

no ipv6 traffic-filter enable-deny-logging [**hw-drop**]

Command Default

Logs are not generated for IPv6 packets that are denied by an ACL.

Parameters

hw-drop

Drops the denied IPv6 packets in hardware.

Modes

Interface configuration mode

Usage Guidelines

IPv6 ACL logging is not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.

This command is supported for LAG ports, with a CAM index created only on the primary port.

By default, any IPv6 packets received on an interface that are denied by an ACL are discarded by the software. To avoid high CPU usage when you enable the log generation of denied IPv6 packets, configure the optional **hw-drop** keyword to drop the IPv6 packets in the hardware after the log is generated.

The **no** form of this command disables the log generation of denied IPv6 packets.

Examples

The following example creates an ACL to deny packets and enables the generation of IPv6 packet logging on Ethernet interface 1/1.

```
device# configure terminal
device(config)# ipv6 access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 traffic-filter deny-log in
device(config-if-e1000-1/1)# ipv6 traffic-filter enable-deny-logging
```

The following example creates an ACL to deny packets, enables the generation of IPv6 packet logging on Ethernet interface 1/1 and drops the packets in hardware.

```
device# configure terminal
device(config)# ipv6 access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 traffic-filter deny-log in
device(config-if-e1000-1/1)# ipv6 traffic-filter enable-deny-logging hw-drop
```

The following example configures the LAG.

```
device(config)#lag  lag1 static id 1
device(config-lag-lag1)#ports Ethernet 1/1 to 1/4
device(condfig-lag-lag1)#primary Ethernet 1/1
device(config-lag-lag1)#deploy

device(config-if-e1000-1/1)#ipv6 traffic-filter deny-log in
device(config-if-1/1)#ipv6 traffic-filter enable-deny-logging hw-drop
```

History

Release version	Command history
5.9.00a	This command was introduced.

ipv6 traffic-filter enable-permit-logging

Generates logs for a specific interface that contain IPv6 packets that are permitted as a result of an access-control list (ACL).

Syntax

ipv6 traffic-filter enable-permit-logging [**selective**]

no ipv6 traffic-filter enable-permit-logging [**selective**]

Command Default

Logs are not generated for IPv6 packets that are permitted by an ACL.

Parameters

selective

Configures logging of permitted traffic to include only the first packet in each time cycle.

Modes

Interface configuration mode

Usage Guidelines

To avoid high CPU usage under permit log generation, include the **selective** keyword.

IPv6 ACL logging is not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.

This command is supported for LAG ports, with a CAM index created only on the primary port.

The **no** form of this command disables the log generation of permitted IPv6 packets.

Examples

The following example creates an ACL with a permit rule, enables the generation of IPv6 packet logging on Ethernet interface 1/1, and binds the ACL to that interface.

```
device# configure terminal
device(config)# ipv6 access-list test1
device(config-ipv6-access-list test1)# permit ipv6 any any log
device(config-ipv6-access-list test1)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 traffic-filter enable-permit-logging
device(config-if-e1000-1/1)# ipv6 traffic-filter test1 in
```

The following example sets the **ipv6 session-logging-age** parameter to 7 minutes and—for IPv6 ACLs—configures permit logging on the device as selective.

The following example sets the ipv6 session parameter to 8 minutes, creates an ACL to permit packets, configures permit logging on Ethernet interface 1/1 as selective, and binds the ACL to that interface.

```
device# configure terminal
device(config)# ipv6 session 8
device(config)# ipv6 access-list test2
device(config-ipv6-access-list test2)# permit ipv6 any any log
device(config-ipv6-access-list test2)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 traffic-filter enable-permit-logging selective
device(config-if-e1000-1/1)# ipv6 traffic-filter test2 in
```

History

Release version	Command history
6.0.00a	This command was introduced.

ipv6 vrrp vrid

Configures an IPv6 Virtual Router Redundancy Protocol (VRRP) virtual router identifier (VRID).

Syntax

ipv6 vrrp vrid *vrid*

no ipv6 vrrp vrid *vrid*

Command Default

An IPv6 VRRP VRID does not exist.

Parameters

vrid

Configures a number for the IPv6 VRRP VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that IPv6 VRRP is enabled globally; otherwise, an error stating "Invalid input..." is displayed as you try to create a VRRP instance.

The **no** form of this command removes the IPv6 VRRP VRID from the configuration.

Examples

The following example configures IPv6 VRRP VRID 1.

```
device# configure terminal
device(config)# ipv6 router vrrp
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 address fd2b::2/64
device(config-if-e1000-1/5)# ipv6 vrrp vrid 2
device(config-if-e1000-1/5-vrid-2)# owner
device(config-if-e1000-1/5-vrid-2)# ipv6-address fe80::768e:f8ff:fe2a:0099
device(config-if-e1000-1/5-vrid-2)# ipv6-address fd2b::2
device(config-if-e1000-1/5-vrid-2)# activate
```

ipv6 vrrp-extended vrid

Configures an IPv6 Virtual Router Redundancy Protocol Extended (VRRP-E) virtual router identifier (VRID).

Syntax

ipv6 vrrp-extended vrid *vrid*

no ipv6 vrrp-extended vrid *vrid*

Command Default

An IPv6 VRRP-E VRID does not exist.

Parameters

vrid

Configures a number for the IPv6 VRRP-E VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that IPv6 VRRP-E is enabled globally; otherwise, an error stating “Invalid input...” is displayed as you try to create a VRRP-E instance.

The **no** form of this command removes the IPv6 VRRP-E VRID from the configuration.

Examples

The following example configures IPv6 VRRP-E VRID 2.

```
device# configure terminal
device(config)# ipv6 router vrrp-extended
device(config-ipv6-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 address fd4b::2/64
device(config-if-e1000-1/5)# ipv6 vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup  priority 50 track-priority 10
device(config-if-e1000-1/5-vrid-2)# ipv6-address fe80::768e:f8ff:fe3a:0099
device(config-if-e1000-1/5-vrid-2)# ipv6-address fd4b::99
device(config-if-e1000-1/5-vrid-2)# activate
```

isis auth-check

Enables authentication checking for an IS-IS interface.

Syntax

isis auth-check [**level-1** | **level-2**]

no isis auth-check [**level-1** | **level-2**]

Command Default

ISIS authentication checking is enabled by default.

Parameters

level-1

Specifies Level 1 packets.

level-2

Specifies Level 2 packets.

Modes

Interface subtype configuration mode

Usage Guidelines

ISIS authentication checking is enabled by default. If either level-1 or level-2 are not specified, the configuration is applied to both Level 1 and Level 2. The **no** form of the command disables IS-IS authentication checking.

Examples

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

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# no isis auth-check
```

The following example re-inables IS-IS authentication checking for Level 2 packets for an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis auth-check
```

isis auth-key

Configures an authentication key for a specified IS-IS interface.

Syntax

isis auth-key *string* [**level-1** | **level-2**]

no isis auth-key *string* [**level-1** | **level-2**]

Command Default

Disabled.

Parameters

string

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

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Interface subtype configuration mode

Usage Guidelines

The authentication mode must be configured on the interface using the **isis auth-mode** command before a *string* can be configured. If the authentication mode is reset, the authentication key must also be reset.

If either level-1 or level-2 are not specified, the configuration is applied to both level-1 and level-2.

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

Examples

The following example configures an authentication key for Level 1 packets on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis auth-key mykey level-1
```

isis auth-mode

Specifies the type of authentication used for an IS-IS interface.

Syntax

isis auth-mode { **cleartext** | **md5** } [**level-1** | **level-2**]

no isis auth-mode { **cleartext** | **md5** } [**level-1** | **level-2**]

Command Default

Disabled.

Parameters

cleartext

Specifies clear text authentication.

md5

Specifies message Digest 5 (MD5) authentication.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Interface subtype configuration mode

Usage Guidelines

If the **level-1** or **level-2** parameter are not used, the configuration is applied to both Level 1 and Level 2 pakcets.

The **no** form of the command removes the configured authentication mode.

Examples

The following example specifies that MD5 authentication is performed on Level 2 packets on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis auth-mode MD5 level-2
```

isis bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific IS-IS interface.

Syntax

isis bfd disable

no isis bfd

Command Default

BFD is disabled by default.

Parameters

disable

Disables BFD on the IS-IS interface.

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated if BFD is enabled globally using the **bfd all-interfaces** command in IS-IS router configuration mode. If BFD is disabled using the **no bfd all-interfaces** command in IS-IS router configuration mode, BFD sessions on specific IS-IS interfaces are deregistered.

The **no** form of the command removes all BFD sessions from a IS-IS specified interface.

Examples

The following example enables BFD on a specific IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis bfd
```

The following example disables BFD on a specific IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis bfd disable
```

isis circut-type

Configures the type of adjacency used for an Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis circut-type { **level-1** | **level-1-2** | **level-2** }

no circut-type { **level-1** | **level-1-2** | **level-2** }

Command Default

Level 1 and Level 2 adjacency is configured by default.

Parameters

level-1

Specifies Level 1 packets only.

level-1-2

Specifies Level 1 and Level 2 packets.

level-2

Specifies Level 2 packets only.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command resets the type of adjacency to the default value of Level 1 and Level 2 adjacency.

Examples

The following example configures Level 1 adjacency on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis circut-type level-1
```

isis hello padding

Re-enables Intermediate System-to-Intermediate System (IS-IS) hello padding at the interface level.

Syntax

isis hello padding

no isis hello padding

Command Default

IS-IS hello padding is enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Generally, you do not need to disable padding unless a link is experiencing slow performance. If you enable or disable padding on an interface, the interface setting overrides the global setting configured using the **hello padding** command.

The **no** form of the command disables hello padding.

Examples

The following example re-enables IS-IS hello padding on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis hello padding
```

isis hello-interval

Specifies how often an IS-IS interface sends hello messages to its IS-IS neighbors.

Syntax

isis hello-interval *value* [**level-1** | **level-2**]

no isis hello-interval *value* [**level-1** | **level-2**]

Command Default

Disabled.

Parameters

value

Specifies the interval. Valid values range from 1 through 63 seconds. The default is 10.

level-1

Configures the hello interval for Level 1 only.

level-2

Configures the hello interval for Level 2 only.

Modes

Interface subtype configuration mode

Usage Guidelines

If you do not use specify the **level-1** or **level-2** parameter, the changes apply to both levels.

The **no** form of the command restores the default of 10 seconds.

Examples

The following example changes the hello interval for Level 1 packets to 20 on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis hello-interval 20 level-1
```

The following example changes the hello interval for Level 1 and Level 2 packets to 40 on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis hello-interval 40
```

isis hello-multiplier

Specifies the number of IS-IS hello packets a neighbor must miss before a device declares adjacency as down.

Syntax

isis hello-multiplier *multiplier* [**level-1** | **level-2**]

no isis multiplier *multiplier* [**level-1** | **level-2**]

Command Default

The default is 3.

Parameters

multiplier

Specifies the multiplier. Valid values range from 3 through 1000. The default is 3.

level-1

Configures the hello multiplier for Level 1 adjacencies.

level-2

Configures the hello multiplier for Level 2 adjacencies.

Modes

Interface subtype configuration mode

Usage Guidelines

The hello multiplier is the number by which an IS-IS interface multiplies the hello interval to obtain the hold time for Level-1 and Level-2 IS-to-IS hello PDUs.

If you do not use specify the **level-1** or **level-2** parameter, the changes apply to both levels.

The **no** form of the command restores the default of 10 seconds.

Examples

The following example changes the hello multiplier for Level 1 packets Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis hello-multiplier 10 level-1
```

The following example changes the hello interval for Level 1 and Level 2 packets to 40 on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis hello-multiplier
```

isis ipv6 metric

Configures the metric value for an interface under IPv6 IS-IS MT.

Syntax

isis ipv6 metric *metric* [**level-1** | **level-2**]

no isis ipv6 metric *metric* [**level-1** | **level-2**]

Command Default

The default is 10.

Parameters

level-1

Specifies Level 1 only.

level-2

Specifies Level 2 only.

multiplier

Specifies the metric value. Valid values range from 1 through 16777215. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

Each IS-IS interface has a separate metric value. In IPv6 IS-IS MT, different metrics are configured on an interface for IPv4 and IPv6. When the metric value is configured for an interface, it rebuilds the route LSP and triggers IPv6 IS-IS MT SPF calculation.

The **no** form of the command restores the default of 10.

Examples

The following example changes the metric value for Level 1 packets for an interface under IPv6 IS-IS MT for an Ethernet interface to 25.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis ipv6 metric 25 level-1
```

The following example changes the metric value for Level 2 packets for an interface under IPv6 IS-IS MT for a loopback interface to 60.

```
device# configure terminal
device(config)# interface loopback 1
device(config-lbif-1)# isis ipv6 metric 60 level-2
```

isis metric

Configures the value of an IS-IS metric.

Syntax

isis metric *metric* [**level-1** | **level-2**]

no isis metric *metric* [**level-1** | **level-2**]

Command Default

The default is 10.

Parameters

metric

Specifies the metric. Valid values range from 1 through 63 for the narrow metric style (the default metric style for IPv4 ISIS). Valid values range from 1 through 16777215 for the wide metric style (the default metric style for IPv4 ISIS).

level-1

Specifies Level 1 only.

level-2

Specifies Level 2 only.

Modes

Interface subtype configuration mode

Usage Guidelines

Each IS-IS interface has a separate metric value.

The device applies the interface-level metric to routes originated on the interface and when calculating routes. The device does not apply the metric to link-state information received from one IS and flooded to other ISs.

If the metric value you want to use is higher than 63 but you have not changed the metric style to wide, you must change the metric style first, then set the metric. The IS-IS neighbors that receive the advertisements must also be enabled to receive wide metrics.

The **no** form of the command restores the default of 10.

Examples

The following example changes the metric for an Ethernet interface, specifying Level 1 packets.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis metric level-1 25
```

isis passive

Disables adjacency formation and advertisements on an Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis passive

no isis passive

Command Default

Adjacency formation and advertisements is disabled on loopback interfaces. Adjacency formation and advertisements is enabled on all other interfaces.

Modes

Interface subtype configuration mode

Usage Guidelines

A device advertises an IS-IS interface to its area regardless of whether adjacency formation is enabled.

The **no** form of the command re-enables adjacency formation and advertisements on the IS-IS interface.

Examples

The following example disables adjacency formation and advertisements on an Ethernet interface.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2)# isis passive
```

The following example enables adjacency formation and advertisements on a loopback interface.

```
device#configure terminal
device(config)# interface looback 1
device(config-lbif-1)# isis passive
```

isis point-to-point

Configures the network type for the Intermediate System-to-Intermediate System (IS-IS) interface as point-to-point.

Syntax

isis point-to-point

no isis point-to-point

Command Default

Disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command removes the configured point-to-point network type.

Examples

The following example configures a network type of point-to-point for an Ethernet interface.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2)# isis point-to-point
```

isis priority

Determines the priority of the interface for being elected as a Designated IS.

Syntax

isis priority *value* [**level-1** | **level-2**]

no isis priority *value* [**level-1** | **level-2**]

Command Default

The default is 64.

Parameters

value

Specifies the priority. Valid values range from 0 through 127. The default is 64.

level-1

Sets the priority for Level 1 only.

level-2

Sets the priority for Level 2 only.

Modes

Interface subtype configuration mode

Usage Guidelines

You can configure the same priority for both Level-1 and Level-2 or you can configure a different priority for each level. If two or more devices have the highest priority within a given level, the device with the highest MAC address becomes the Designated IS for that level.

You can set the IS-IS priority on an individual interface basis only. You cannot set the priority globally.

The **no** form of the command restores the default of 64.

Examples

The following example changes the priority for Level 1 packets for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis priority 100 level-1
```

The following example changes the hello multiplier for Level 2 packets for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-lbif-1)# isis priority 80 level-2
```

isis reverse-metric

Configures the reverse metric value on a single Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

no isis reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

Command Default

Disabled.

Parameters

value

Specifies the reverse metric value in metric style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default value is 16777214 irrespective of the metric style configured.

whole-lan

Specifies that the configured reverse metric value affects the entire LAN.

te-def-metric

Specifies that the device sends a traffic engineering (TE) default metric sub-type-length-value (TLV) within the reverse metric TLV.

Modes

Interface subtype configuration mode

Usage Guidelines

If the reverse metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor routdeviceer receives the reverse metric value through the IS hello, the neighbor router updates the cost to reach the original IS-IS router with the sum of default metric and the reverse metric value. This helps in shifting traffic to the other alternate paths.

If the **whole-lan** option is not enabled, the reverse metric value affects only the neighbor router. The **whole-lan** option takes effect only on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the **whole-lan** option is enabled.

The **no** form of the command removes the entire reverse metric configuration. The **no** form of the command specified with the configured value resets the metric value to the default value of 16777214.

NOTE

The **isis reverse-metric** *value* command is supported on the Brocade NetIron XMR Series, the Brocade MLX Series, and the Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

Examples

The following example configures a reverse metric value of 40 on an Ethernet interface. The **whole-lan** option is enabled to include the entire LAN.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2)# isis reverse-metric 40 whole-lan
```

History

Release version	Command history
5.7.00	This command was introduced.

is-type

Changes the Intermediate System-to-Intermediate System (IS-IS) level globally.

Syntax

is-type { **level-1** | **level-1-2** | **level-2** }

no is-type { **level-1** | **level-1-2** | **level-2** }

Command Default

The device operates as both a Level 1 (intra-area) and a Level 2 (interarea) device.

Parameters

level-1

Specifies that the device performs only Level 1 (intra-area) routing.

level-1-2

Specifies that the device performs both Level 1 and Level 2 routing.

level-2

Specifies that the device performs only Level 2 (interarea) routing.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command enables support for both IS-IS levels, if one level has been disabled. Alternatively, the **level-1-2** parameter can be used.

Examples

The following example changes the IS-IS level globally to Level-1 only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-1
```

The following example changes the IS-IS level globally to Level-2 only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-2
```

The following example changes the IS-IS level globally to Level-1 and Level-2 if support for one level has previously been disabled.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-1-2
```

jitc enable

Enables the Joint Interoperability Test Command (JITC) mode.

Syntax

jitc enable

no jitc enable

Command Default

JITC is not enabled.

Modes

Global configuration mode.

Usage Guidelines

When JITC is enabled, the Advanced Encryption Standard - Cipher-Block Chaining (AES-CBC) encryption mode for the Secure Shell (SSH) protocol is disabled and the AES-CTR (Counter) encryption mode is enabled. To enable the AES-only mode for SSH, use the **ip ssh encryption aes-only** command. To disable the AES-CBC encryption mode, use the **ip ssh encryption disable-aes-cbc** command. When the **jitc enable** command is configured, the **ip ssh encryption aes-only** command and the **ip ssh encryption disable-aes-cbc** command are automatically enabled.

When JITC is enabled, the MD5 authentication scheme for NTP is disabled. The SHA1 authentication scheme is available to define the authentication key for NTP.

The **no** form of the command disables the JITC mode and puts the system back to the standard mode and enables both AES-CBC encryption mode and MD5 authentication configuration. The **ip ssh encryption disable-aes-cbc** command is removed from the running configuration. The **ip ssh encryption aes-only** command configuration is retained in the running configuration.

Examples

The following example enables the JITC mode.

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

In the output below, when the JITC mode is configured, the running configuration displays MD5 as disabled. The **ip ssh encryption aes-only** command and the **ip ssh encryption disable-aes-cbc** command are enabled. The commands are highlighted below.

NOTE

In the output below, the authentication-key entry is displayed when the authentication key for NTP is configured separately.

```
device(config)# show run | begin jitc
!
jitc enable
!
ntp
 disable authenticate md5
 authentication-key key-id 1 sha1 2 $b24tb25V
!
ip ssh encryption aes-only
ip ssh encryption disable-aes-cbc

end
```

History

Release version	Command history
5.8.00	This command was introduced.

Commands K - Sh

ka-int-count

Configures the number of keepalive intervals after which the session is terminated when no session keepalive or other LDP protocol message is received from the LDP peer.

Syntax

ka-int-count *number*

no ka-int-count *number*

Command Default

The default is a count of six intervals.

Parameters

number

Specifies the number of keepalive time intervals. Enter an integer from 1 to 65535.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default count of six intervals.

Examples

The following example configures a keepalive interval count of three.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# ka-int-count 3
```

ka-interval

Sets the keepalive time interval at which the session keepalive message is sent when no other LDP protocol message is sent to the LDP peer.

Syntax

ka-interval *seconds*

no ka-interval *seconds*

Command Default

The default is six seconds.

Parameters

seconds

Specifies the keepalive time interval in seconds. Enter an integer from 1 to 65535.

Modes

MPLS LDP configuration mode

Usage Guidelines

The **ka-interval** and the **ka-timeout** configurations are mutually exclusive and you may have only one configured at a time. You must explicitly remove the configuration for one in order to change to the other configuration.

When the keepalive timeout value is configured, the **show mpls ldp** command displays keepalive interval as keepalive timeout divided by the keepalive interval count (ka-timeout/ka-in-count).

A message is displayed whenever the **ka-interval** value is changed.

```
"Please clear LDP sessions for the new KA parameter value to take effect on existing sessions"
```

Use the **no** form of the command to reset the default of six seconds.

Examples

The following example configures a keepalive interval of 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# ka-interval 10
```

ka-timeout

Sets the keepalive timeout after which the session is terminated when the keepalive or LDP protocol message is not received.

Syntax

ka-timeout *seconds*

no ka-timeout *seconds*

Command Default

The default is six seconds.

Parameters

seconds

Specifies the keepalive timeout in seconds. Enter an integer from 1 to 65535.

Modes

MPLS LDP configuration mode

Usage Guidelines

After an LDP session is established, an LSR maintains the integrity of the session by sending keepalive messages. The keepalive timer for each peer session resets whenever it receives any LDP protocol message or a keepalive message on that session. When the keepalive timer expires, LDP concludes that the TCP connection is bad or the peer is dead and terminates the session.

When the keepalive timeout value is configured, the **show mpls ldp** command displays keepalive interval as keepalive timeout divided by the keepalive interval count (ka-timeout/ka-in-count).

The **ka-interval** and the **ka-timeout** configurations are mutually exclusive and you may have only one configured at a time. You must explicitly remove the configuration for one in order to change to the other configuration.

A message is displayed whenever the **ka-timeout** value is changed.

```
"Please clear LDP sessions for the new KA parameter value to take effect on existing sessions"
```

Use the **no** form of the command to reset the default timeout of six seconds.

Examples

The following example configures a keepalive timeout of 180 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# ka-timeout 180
```

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*

Command Default

The interval is 300 seconds.

Parameters

interval

Specifies the add-remove interval in seconds. Valid values range from 0 through 14400. The default is 300.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command sets 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-ospf6-router)# key-add-remove-interval 240
```

The following example sets the key add-remove interval to 210 seconds in a nondefault VRF instance:

```
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ospf6-router-vrf-red))# key-add-remove-interval 240
```

key-rollover-interval

Alters the timing of the existing configuration changeover.

Syntax

key-rollover-interval *interval*

no key-rollover-interval *interval*

Command Default

The interval is 300 seconds.

Parameters

interval

Specifies the key-rollover-interval in seconds. Valid values range from 0 through 14400. The default is 300.

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 sets 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-ospf6-router)# 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-ospf6-router)# no key-rollover-interval 420
```

The following example re-sets the key rollover interval to the default value in a nondefault VRF instance.

```
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ospf6-router-vrf-red))# no key-rollover-interval 420
```

key-server-priority

Configures the MACsec key-server priority for the MACsec Key Agreement (MKA) group to select key server.

Syntax

key-server-priority *value*

no key-server-priority *value*

Command Default

Key-server priority is set to 16. This is not displayed in configuration details.

Parameters

value

Specifies key-server priority. The possible values range from 0 to 255, where 0 is highest priority and 255 is lowest priority. Default is 16.

Modes

dot1x-mka-cfg-group mode.

Usage Guidelines

During key-server election, the server with the highest priority (the server with the lowest key-server priority value) becomes the key-server.

The **no** form of the command removes the previous priority setting.

Examples

The following example explains how to set the key-server priority for MKA group group1 to 20.

```
deviceenable
deviceconfigure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# key-server-priority 20
```

History

Release version	Command history
5.8.00	This command was introduced.

l2 policy route-map

Enables Layer 2 PBR by applying a route map that is configured for Layer 2 PBR on an interface.

Syntax

l2 policy route-map *route-map-name*

no l2 policy route-map *route-map-name*

Command Default

Layer 2 PBR is not enabled by default.

Parameters

route-map-name

Specifies the name of the route map to be applied on the physical interface.

Modes

Interface configuration mode.

Usage Guidelines

Layer 2 PBR cannot be applied globally. Layer 2 PBR can be applied only at the physical interface level.

If both Layer 2 PBR and Layer 3 PBR are applied on the same interface (or Layer 3 PBR is applied globally), Layer 2 PBR only filters non-IP packets. If only Layer 2 PBR is applied, Layer 2 PBR filters both IP and non-IP packets.

Layer 2 PBR cannot be applied on a VE interface.

Layer 2 PBR cannot be applied on an interface where Layer 2 ACL or Layer 3 ACL is already applied.

Layer 2 PBR cannot be applied on an interface where ACL-based rate limiting is already applied.

The **no** form of the command removes the route map applied on the interface.

Examples

The following example enables Layer 2 PBR by applying a route map that is configured for Layer 2 PBR on an interface.

```
deviceenable
deviceconfigure terminal
device(config)# mac access-list abc
device(config-mac-acl-abc)# permit any any any etype 8000
device(config-mac-acl-abc)# exit

device(config)# route-map pbr permit 1
device(config-routemap pbr)# match l2acl abc
device(config-routemap pbr)# set next-hop-flood-vlan 100
device(config-routemap pbr)# exit

device(config) interface ethernet 1/1
device(config-if-e10000-1/1)# l2 policy route-map pbr
```

History

Release version	Command history
5.8.00b	The command was introduced.

label-range static

Configures the minimum and maximum values for user-configurable static labels.

Syntax

label-range static { **min-value** *num* | **max-value** *num* }

no label-range static { **min-value** *num* | **max-value** *num* }

Parameters

min-value

Denotes the lower end of the range for the static labels.

num

The range designation and can be between 16 - 499999. The default value is 16.

max-value

Denotes the top end of the range for the static labels.

num

The range designation and can be between 16 - 499999. The default value is 2047.

Modes

MPLS router mode (config-mpls).

Usage Guidelines

Labels are automatically distributed using LDP, RSVP or BGP. If a LSR is connected to a device that supports MPLS forwarding but does not support LDP, static labels can be used to maintain forwarding.

LDP, RSVP or BGP can be used to dynamically distribute label bindings. After an LSR receives labels, it installs the bindings into the *Label Forwarding Information Base (LFIB)* for MPLS forwarding.

- Static labels to IPv4 prefix binding
- Static cross-connects of labels
- To configure static label binding, define a static label range
- Cannot configure static labels for IPv4 VPN prefixes
- Bindings remain in LFIB even if the next hop LSR is down

The **no** form of the command restores the default to 16 for the min-value and to 2047 for max-value.

Examples

The following example displays the **label-range static** command:

```
deviceconfigure terminal
device(config)# router-mpls
device(config-mpls)# label-range static min 16 max 2047
```

key-rollover-interval

Alters the timing of the existing configuration changeover.

Syntax

key-rollover-interval *interval*

no key-rollover-interval *interval*

Command Default

The interval is 300 seconds.

Parameters

interval

Specifies the key-rollover-interval in seconds. Valid values range from 0 through 14400. The default is 300.

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 sets 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-ospf6-router)# 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-ospf6-router)# no key-rollover-interval 420
```

The following example re-sets the key rollover interval to the default value in a nondefault VRF instance.

```
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ospf6-router-vrf-red))# no key-rollover-interval 420
```

label-withdrawal-delay

Delays sending a label withdrawal message for a FEC to a neighbor in order to allow the IGP and LDP to converge.

Syntax

label-withdrawal-delay *secs*

no label-withdrawal-delay *secs*

Command Default

The default is 60.

Parameters

secs

Specifies the delay period in seconds for the label withdrawal delay timer. Enter value from 0 to 300.

Modes

MPLS LDP configuration mode.

Usage Guidelines

Setting the *secs* variable to zero (0) disables the feature for subsequent events.

Setting the *secs* variable to a value from 1 to 300, updates the configured value.

When using the **no** form of the command to restore the default behavior, the specified value for the *secs* variable must match the configured value at the time that the **no** form of the command executes.

Examples

The following example sets the label withdrawal delay timer to 30 seconds.

```
device(config-mpls-ldp)# label-withdrawal-delay 30
```

The following example restores the command default behavior when the delay period configuration is already 30 seconds.

```
device(config-mpls-ldp)# no label-withdrawal-delay 30
```

The following example disables the label withdrawal delay timer.

```
device(config-mpls-ldp)# label-withdrawal-delay 0
```

History

Release	Command history
5.5.00	This command is introduced.

lacp system-priority

Configures the Link Aggregation Control Protocol (LACP) system priority in a dynamic or keep-alive LAG at the global configuration level.

Syntax

lacp system-priority *number*

no lacp system-priority *number*

Command Default

The LACP system priority is not configured.

Parameters

number

Specifies the value of the LACP system priority. Valid values are from 1 through 65535. The default system-priority value is 1.

Modes

Global configuration mode

Usage Guidelines

This configuration is only applicable for configuration of a dynamic or keep-alive LAGs. The **no** form of the command removes the LACP system priority in the LAG.

NOTE
In a system configuration with multiple MCT peers, the LACP system priority on both the MCT nodes should be the same.

Examples

The following example configures the LACp system priority as 4.

```
device(config)# lacp system-priority 4
```

lag port-primary-dynamic

Enables the user to dynamically select the primary port in a link aggregation group (LAG) at the global configuration level without bringing down the LAG.

Syntax

lag port-primary-dynamic

no lag port-primary-dynamic

Command Default

The primary port in a LAG is not dynamically selected.

Modes

Global configuration mode

Usage Guidelines

This command works for static or dynamic LAGs and is available on Brocade NetIron MLX devices only. The **no** form of the command disables the feature to dynamically select the primary port in a LAG. Use the **show running-configuration** command to verify that the primary port has been changed on the LAG.

To find the full description of dynamic port selection, including the prerequisites and limitations, refer to the specific chapter and topics in the *NetIron Switching Configuration Guide*.

NOTE
The **lag port-primary-dynamic** command supports dynamic selection of a primary port if Layer 3 configurations are configured in the virtual interface (VE). The command does not support Layer 2 configurations.

Examples

The following example enables dynamic selection of the primary port in a LAG at the global configuration level.

```
device(config)# lag port-primary-dynamic
```

History

Release version	Command history
6.0.00a	This command was introduced.

ldp

Enables the Label Distribution Protocol (LDP) mode to configure LDP global parameters.

Syntax

ldp

no ldp

Modes

MPLS configuration mode

Usage Guidelines

Use the **no** form of this command to remove the LDP configurations from the device.

Examples

The following example enables LDP configuration mode.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# ldp
```

ldp-enable

Enables LDP on an interface.

Syntax

ldp-enable

no ldp-enable

Command Default

None

Modes

MPLS interface configuration mode

Usage Guidelines

For an LDP session between routers, you must configure LDP on an interface to allow the device to advertise its loopback interface to the peers.

To use LDP, configure a loopback address with a 32-bit mask on the LSR. The first loopback address configured on the device is used in its LDP identifier. When the loopback address used in the LDP identifier is removed, all LDP functions on the LSR are shut down. LDP sessions between the LSR and its peers are terminated, and LDP-created tunnels are removed. When other loopback interfaces are configured on the device, the lowest-numbered loopback address is used as a new LDP identifier. LDP sessions and tunnels are set up using this new LDP identifier.

Configure LDP on the same set of interfaces that IGP routing protocols such as OSPF and IS-IS are enabled.

Use the **no** form of the command to disable LDP on the interface.

Examples

The following example configures LDP on an interface.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# mpls-interface ethernet 1/2
device(config-mpls-if-e-1/2)# ldp-enable
```

ldp-params

Allow you to access ldp-params subconfiguration mode to configure LDP parameters on an interface.

Syntax

ldp-params

no ldp-params

Command Default

None

Modes

MPLS interface configuration mode

Usage Guidelines

When you use this command, you can configure the LDP Hello interval and timeout parameters on the interface.

Use the **no** form of the command to remove the LDP parameter configuration.

Examples

The following example accesses ldp-params subconfiguration mode.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# mpls-interface ethernet 1/2
device(config-mpls-if-e100-1/2)# ldp-params
device(config-mpls-if-e100-1/2-ldp-params)#
```

ldp-sync

Enables Multiprotocol Label Switching (MPLS) Label Distribution Protocol-Interior Gateway Protocol (LDP-IGP) synchronization globally with Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), and configures the hold-down time interval.

Syntax

ldp-sync [**hold-down** *seconds*]

no ldp-sync [**hold-down**]

Command Default

Disabled.

Parameters

hold-down *seconds*

Sets the LDP-IGP synchronization hold-down time interval in seconds. The IGP must advertise the maximum IP metric while waiting for an update from the LDP. Valid values range from 1 through 65535 seconds. The default is 30.

Modes

OSPF router configuration mode

IS-IS address-family IPv4 unicast configuration mode

Usage Guidelines

The **ldp-sync** command supports point-to-point interfaces, but not tunnel interfaces.

This command affects IPv4 metrics only.

When enabled on IS-IS, consider the following:

- The feature applies to both level-1 and level-2 metrics.
- The wide metric-style is required.

The **no ldp-sync** command disables LDP-IGP synchronization.

The **no ldp-sync hold-down** command resets the hold down time interval to the default setting of 30 seconds.

Examples

The following example enables MPLS LDP-IGP synchronization globally with OSPF and IS-IS, and sets the hold-down time interval to 100 seconds.

```
device(config)# router ospf
device(config-ospf-router)# ldp-sync
device(config-ospf-router)# ldp-sync hold-down 100
device(config-ospf-router)# exit
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-isis-router-ipv4u)# metric-style wide
device(config-isis-router-ipv4u)# ldp-sync
device(config-isis-router-ipv4u)# ldp-sync hold-down 100
```

License add

Installs the license file to the device.

Syntax

license add { **license file.xml** }

Parameters

license file.xml

Specifies the license file to be installed on the flash.

Modes

Privilege EXEC level.

Usage Guidelines

Use this command to install the license to the device after the file is copied to the MP flash directory. To copy the license file to the MP flash directory, use the **copy tftp flash** command. Once the file is copied to the directory, use the **license add** command to install the license to the device.

The command is not enabled by default.

Examples

The following example installs the 10x10-20PUPG license to upgrade the system from 10-port to 20-port.

```
device# license add 20150831003730756eydFIJM1FFr.xml
```

History

Release version	Command history
05.0.00	This command was introduced.

license delete

Removes the license file from the license database.

Syntax

license delete *index_number*

Parameters

index_number

The index_number variable is a valid license index number. The license index number can be retrieved from the **show license** command output.

Modes

Privileged EXEC level.

Usage Guidelines

The licensed feature will continue to run as configured until the software is reloaded, at which time the feature will be disabled and removed from the system. Syslog and trap messages are generated when the license is deleted.

Examples

The following example shows the command will remove the license for index number 7.

```
device# license delete 7
```

History

Release version	Command history
05.0.00	This command was introduced.

link-protection

Enables link protection for an FRR enabled LSP.

Syntax

link-protection

no link-protection

Command Default

The default configuration is always node protection.

Modes

FRR-LSP mode (config-mpls-lsp-frr).

Usage Guidelines

The **no** function of the command sets protection type back to default behavior, which is node protection.

Examples

The following example displays the configuration example for an adaptive LSP:

```
device#configure terminal
device(config)# router mpls
device(config-mpls)# lsp t1
device(config-mpls-lsp-t1)# to 44.44.44.44
device(config-mpls-lsp-t1)# frr
device(config-mpls-lsp-t1-frr)# link-protection
device(config-mpls-lsp-t1)# enable
```

The following example displays the configuration example for a non-adaptive LSP:

```
device#configure terminal
device(config)# router mpls
device(config-mpls)# lsp t1
device(config-mpls-lsp-t1)# to 44.44.44.44
device(config-mpls-lsp-t1)# adaptive
device(config-mpls-lsp-t1)# enable
device(config-mpls)# lsp t1
device(config-mpls-lsp-t1)# frr
device(config-mpls-lsp-t1-frr)# link-protection
device(config-mpls-lsp-t1)# commit
```

History

Release	Command history
5.6.00	This command is introduced.

link-redundancy

Enables VSRP link-redundancy mode.

Syntax

link-redundancy

no link-redundancy

Command Default

VSRP link redundancy is not enabled.

Modes

VSRP VRID configuration mode

Usage Guidelines

After enabling link redundancy, VSRP switches to master-confirm state and the backup state creates a link redundant port list.

VSRP switches that are in initial state and master state don't need to create link redundant port list.

The **no** form of the command disables VSRP link redundancy.

Examples

The following example enables VSRP link redundancy.

```
device(config)# vlan 10
device(config-vlan-10)# vsrp vrid 10
device(config-vlan-10-vsrp-10)# link-redundancy
```

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

Use the **no** form of this command to remove the ASN from the device.

ASNs in the range from 64512 through 65535 are private numbers that are not advertised to the external community.

Examples

This example assigns a separate local AS number.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# local-as 777
```

load-balance mask ip

Masks specific values during ECMP and LAG index hash calculations.

Syntax

load-balance mask ip [**dst-ip** [*slot number* | **all** | **pre-symmetriclb**] | **src-ip** [*slot number* | **all** | **pre-symmetriclb**] | **dst-l4-port** |[*slot number* | **all**] | **src-l4-port** [*slot number* | **all**] | **protocol** [*slot number* | **all**]]

no load-balance mask ip [**dst-ip** [*slot number* | **all** | **pre-symmetriclb**] | **src-ip** [*slot number* | **all** | **pre-symmetriclb**] | **dst-l4-port** |[*slot number* | **all**] | **src-l4-port** [*slot number* | **all**] | **protocol** [*slot number* | **all**]]

Command Default

The functionality is disabled by default.

Parameters

dst-ip

Masks the destination IP address.

pre-symmetriclb

Masks the IP address before symmetric load balancing can occur.

slot number

Identifies the slot number for the specific source or destination IP address, TCP or UDP source or destination port, or IPv4 protocol.

all

Applies the command to all ports within the device.

src-ip

Masks the source IP address.

dst-l4-port

Masks the Layer 4 destination port.

src-l4-port

Masks the Layer 4 source port.

protocol

Masks the IPv4 protocol ID.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the masking of specified values during ECMP and LAG index hash calculations.

Examples

The following example masks all the Layer 4 source ports within the device.

```
device(config)# load-balance mask ip src-l4-port all
```

The following example masks the source IP address before symmetric load balancing can occur for the IPv4 traffic entering slot 10 of the device.

```
device(config)# load-balance mask ip src-ip pre-symmetriclb 10
```

History

Release version	Command history
5.4.00	This command was introduced.
5.9.00	This command was modified to include the **pre-symmetriclb** option.

load-balance mask ipv6

Masks specific values during ECMP and LAG index hash calculations for IPv6.

Syntax

load-balance mask ipv6 [**dst-ip** [*slot number* | **all** | **pre-symmetriclb**] | **src-ip** [*slot number* | **all** | **pre-symmetriclb**] | **dst-l4-port** |[*slot number* | **all**] | **src-l4-port** [*slot number* | **all**] | **next-hdr** [*slot number* | **all**]]

no load-balance mask ipv6 [**dst-ip** [*slot number* | **all** | **pre-symmetriclb**] | **src-ip** [*slot number* | **all** | **pre-symmetriclb**] | **dst-l4-port** |[*slot number* | **all**] | **src-l4-port** [*slot number* | **all**] | **next-hdr** [*slot number* | **all**]]

Command Default

The functionality is disabled by default.

Parameters

dst-ip

Masks the destination IPv6 address.

pre-symmetriclb

Masks the IPv6 address before symmetric load balancing can occur.

slot number

Identifies the slot number for the specific source or destination IPv6 address, TCP or UDP source or destination port, or IPv6 protocol.

all

Applies the command to all ports within the device.

src-ip

Masks the source IPv6 address.

dst-l4-port

Masks the Layer 4 destination port.

src-l4-port

Masks the Layer 4 source port.

next-hdr

Masks the IPv6 next header.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables masking of specified values during ECMP and LAG index hash calculations for IPv6.

Examples

The following example masks all the source IPv6 ports within the device.

```
device(config)# load-balance mask ipv6 src-ip all
```

The following example masks the destination IPv6 address before symmetric load balancing can occur for the IPv6 traffic entering on slot 5 of the device.

```
device(config)# load-balance mask ipv6 dst-ip pre-symmetriclb 5
```

History

Release version	Command history
5.4.00	This command was introduced.
5.9.00	This command was modified to include the **pre-symmetriclb** option.

load-sharing

Configures the maximum number of LDP ECMP paths.

Syntax

load-sharing *number*

no load-sharing

Command Default

The default number of ECMP paths is one.

Parameters

number

Specifies the maximum number of LDP ECMP paths. Enter an integer from 1 to 8.

Modes

MPLS LDP configuration mode

Usage Guidelines

The number of LDP ECMP paths for transit LSR depends on the number of eligible paths that are available, and the maximum number of LDP ECMP paths that you can configure.

Use the **no** form of this command to reset the default of one.

Examples

The following example configures a maximum of four LDP ECMP paths.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# load-sharing 4
```

local-certificate

Specifies the URL for the local peer certificate of a specific trustpoint.

Syntax

local-certificate url *URL name*

no local-certificate url *URL name*

Parameters

url

Specifies the URL name for the local peer certificate.

URL name

The URL name for the local peer certificate.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The **no** form of the removes the local certificate URL name.

Examples

The following example specifies the local certificate URL name as provided here.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# local-certificate url http://WIN-HJ98AK136A0.englab.brocade.com/
pki_local_cert
```

History

Release version	Command history
5.9.00	This command was introduced.

location

Configures the location for the Public Key Infrastructure (PKI) entity.

Syntax

location *string*

Parameters

string

Specifies name of the location for PKI entity.

Modes

PKI entity configuration mode

Examples

The following example configures the location for PKI entity.

```
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# location brocade_location
```

History

Release version	Command history
05.8.00	This command was introduced.

log (OSPFv2)

Controls the generation of OSPFv2 logs.

Syntax

log { **adjacency** [**dr-only**] | **all** | **bad_packet** [**checksum**] | **database** | **memory** | **retransmit** }

no log { **adjacency** [**dr-only**] | **all** | **bad_packet** [**checksum**] | **database** | **memory** | **retransmit** }

Command Default

Only OSPFv2 messages indicating possible system errors are logged. Refer to the Parameters section for specific defaults.

Parameters

adjacency

Specifies the logging of essential OSPFv2 neighbor state changes. This option is disabled by default.

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. This option is enabled by default.

checksum

Specifies all OSPFv2 packets that have checksum errors.

database

Specifies the logging of OSPFv2 LSA-related information. This option is disabled by default.

memory

Specifies the logging of OSPFv2 memory issues. This option is enabled by default.

retransmit

Specifies the logging of OSPFv2 retransmission activities. This option is disabled by default.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv2. If this command is not enabled only OSPFv2 messages indicating possible system errors are logged.

For interfaces where the designated router state is not applicable, such as point-to-point and virtual links, OSPF neighbor state changes are always logged irrespective of the setting of the **dr-only** sub-option.

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 the command restores the default settings. Use the **no log all** command to return all OSPFv2 logging options to the default settings.

Examples

The following example enables the logging of all OSPFv2-related syslog events.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# log all
```

The following example enables the logging of OSPFv2 retransmission activities.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# log retransmit
```

logging enable

Enables system log messages and traps for the specified protocol or event.

Syntax

logging enable { **bfd** | **cfm** | **config-changed** | **fan-speed-change** | **fan-state-change** | **ikev2** | **ikev2-extended** | **ipsec** | **link-state-change** | **mac-mismatch-detection** | **mgmt-mod-redun-state-change** | **module-hotswap** | **mpls** | **mvrp-vlan** | **ntp** | **ospf** | **pki-extended** | **rstp** | **snmp-auth-failure** | **temp-error** | **user-login** | **vrrp-config-validate** | **vrrp-if-state-change** }

no logging enable { **bfd** | **cfm** | **config-changed** | **fan-speed-change** | **fan-state-change** | **ikev2** | **ikev2-extended** | **ipsec** | **link-state-change** | **mac-mismatch-detection** | **mgmt-mod-redun-state-change** | **module-hotswap** | **mpls** | **mvrp-vlan** | **ntp** | **ospf** | **pki-extended** | **rstp** | **snmp-auth-failure** | **temp-error** | **user-login** | **vrrp-config-validate** | **vrrp-if-state-change** }

Command Default

Log messages for specific protocols or events are enabled.

Parameters

bfd
Specifies the log messages and traps for BFD.

cfm
Specifies the log messages and traps for CFM.

config-changed
Specifies the log messages and traps for configuration data changed.

fan-speed-change
Specifies the log messages and traps for fan speed change events.

fan-state-change
Specifies the log messages and traps for fan state change events.

ikev2
Specifies the log messages and traps for IKEv2 events.

ikev2-extended
Specifies the extended log messages and traps for IKEv2 events.

ipsec
Specifies the log messages and traps for IPsec events.

link-state-change
Specifies the log messages and traps for link state change events.

mac-mismatch-detection
Enables or disables the Ethernet MAC address and ARP MAC address mismatch detection syslog message.

mgmt-mod-redun-state-change
Specifies the log messages and traps for management module redundant state change events.

module-hotswap
Specifies the log messages and traps for module inserted or removed events.

mpls
Specifies the log messages and traps for MPLS events.

mvrp-vlan
Specifies the log messages and traps for MVRP VLAN events.

ntp
Specifies the log messages and traps for NTP events.

ospf
Specifies the log messages and traps for OSPF events.

pki-extended
Specifies the extended log messages and traps for IKEv2 events.

rstp
Specifies the log messages and traps for RSTP events.

snmp-auth-failure
Specifies the log messages and traps for SNMP authentication failure events.

temp-error
Specifies the log messages and traps for temperature error events.

user-login
Specifies the log messages and traps for login usernames.

vrrp-config-validate
Specifies the log messages and traps for VRRP for configuration validation events.

vrrp-if-state-change
Specifies the log messages and traps for VRRP if state change events.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command disables the generation of the specified syslog messages and traps.

Examples

The following example configures syslog generation for IPsec events.

```
device(config)# logging enable ipsec
```

The following example enables the syslog message to be displayed if there is any source MAC address mismatch between the Layer 2 Ethernet header and the ARP header.

```
device(config)# logging enable mac-mismatch-detection
```

History

Release version	Command history
5.9.00	This command was modified to add the **mac-mismatch-detection** and **vrrp-config-validate** keywords to the syntax.
5.9.00a	This command was modified to add the **ikev2-extended** and **pki-extended** keywords to the syntax.

log adjacency

Logs changes in the status of an adjacency with another intermediate system (IS).

Syntax

log adjacency

no log adjacency

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command disables the logging of adjacency changes.

Examples

The following example enables logging of adjacency changes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# log adjacency
```

The following example disables logging of adjacency changes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no log adjacency
```

log-dampening-debug

Logs dampening debug messages.

Syntax

log-dampening-debug

no log-dampening-debug

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

The following example logs dampening debug messages.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# log-dampening-debug
```

log invalid-lsp-packets

Logs invalid Link State PDUs (LSPs) packets.

Syntax

log invalid-lsp-packets

no log invalid-lsp-packets

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command disables the logging of invalid LSP packets.

Examples

The following example enables logging of invalid LSP packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# log invalid-lsp-packets
```

The following example disables logging of invalid LSP packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no log invalid-lsp-packets
```

log-status-change

Controls the generation of all OSPFv3 logs.

Syntax

log-status-change

no log-status-change

Command Default

Disabled

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of events related to OSPFv3, such as neighbor state changes and database overflow conditions.

The **no** form of this command disables the logging of events.

Examples

The following example disables the logging of events.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# no log-status-change
```

The following example enables the logging of events.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# log-status-change
```

logs-per-interval-per-mep-rmep

Limits the log generation of individual MEPs or RMEPs in a 15 minute time window.

Syntax

logs-per-interval-per-mep-rmep *value*

no logs-per-interval-per-mep-rmep *value*

Command Default

Limiting the log generation for MEPs or RMEPs is not enabled by default.

Parameters

value

Specifies the number of logs generated per MEP or RMEP per 900000 milliseconds. The decimal range is from 1 to 100. The default is 10.

Modes

CFM Protocol Configuration mode.

Usage Guidelines

Use the **logs-per-interval-per-mep-rmep** *value* command to limit the number of logs generated for each MEP or RMEP in a 15 minute time window. When the *value* parameter is configured, the value is uniform for all MEPs and RMEPs. The **no logs-per-interval-per-mep-rmep** *value* command resets the value to the default value.

NOTE
The **logs-per-interval-per-mep-rmep** *value* command is supported on Brocade NetIron XMR Series and Brocade NetIron MLX Series devices, and Brocade NetIron CES Series and Brocade NetIron CER Series devices.

Examples

The following example limits the log generation to 20 logs per MEP or RMEP in a 15 minute time window.

```
device(config)#cfm-enable
device(config-cfm)#logs-per-interval-per-mep-rmep 20
device(config-cfm)#
```

Use the **show cfm logs-limit-per-mep-rmep** command to display the *value* parameter configured for the log limit generation for each MEP or RMEP. The *value* parameter is highlighted in the output.

```
device(config-cfm)# show cfm logs-limit-per-mep-rmep
Logs limit per interval (900000 ms) per MEP/RMEP : 20 (Default : 10)
```

History

Release version	Command history
05.7.00	This command was introduced.

lsp

Accesses LSP subconfiguration mode to configure the LSP tunnel.

Syntax

lsp *name*

no lsp *name*

Command Default

None

Parameters

name

Specifies the name of the LSP tunnel.

Modes

MPLS configuration mode

Usage Guidelines

Use the **no** form of this command to remove the LSP from the MPLS configuration.

Examples

The following example configures LSP to2 and accesses LSP subconfiguration mode.

```
device(config)# router mpls
device(config-mpls)# lsp to2
device(config-mpls-lsp-to2)#
```

lsp-gen-interval

Sets the minimum number of seconds the device waits between sending updated Link State PDUs (LSPs) to its Intermediate System-to-Intermediate System (IS-IS) neighbors.

Syntax

lsp-gen-interval *interval*

lsp-gen-interval *interval*

Command Default

The default interval is 10 seconds.

Parameters

secs

Specifies the interval in seconds. Valid values range from 0 through 120 seconds. The default is 10 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command removes the configured interval.

Examples

The following example changes the LSP generation interval to 45 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-gen-interval 45
```

lsp-interval

Sets the rate of transmission, in milliseconds, of the Link State PDUs (LSPs).

Syntax

lsp-interval *interval*

lsp-interval *interval*

Command Default

The default interval is 33 milliseconds.

Parameters

secs

Specifies the interval in milliseconds. Valid values range from 1 through 4294967295 milliseconds. The default is 33 milliseconds.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command removes the configured interval.

Examples

The following example changes the LSP interval to 45 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-interval 45
```

lsp-refresh-interval

Sets the maximum number of seconds a device waits between sending updated Link State PDUs (LSPs) to its Intermediate System-to-Intermediate System (IS-IS) neighbors.

Syntax

lsp-refresh-interval *interval*

lsp-refresh-interval *interval*

Command Default

The default interval is 900 seconds (15 minutes).

Parameters

secs

Specifies the interval in seconds. Valid values range from 1 through 65535 seconds. The default is 900 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command removes the configured interval.

Examples

The following example changes the LSP refresh interval to 20000 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-refresh-interval 20000
```

lsr-id

Configures an IP address to be used as the LSR ID for the LDP identifier.

Syntax

lsr-id *ip_addr*

no lsr-id *ip_addr*

Command Default

The LSR-ID is the first available loopback interface address.

Parameters

ip_addr

Specifies the IP address to assign to the LSR identifier.

Modes

MPLS LDP configuration mode

Usage Guidelines

You can configure only an IPv4 address.

Use the **no** form of the command to reset the default behavior. When you enter the **no** form of the command and LDP protocol is in the enabled state, the device uses the same LSR-ID until the LDP protocol is disabled; the IP address selected as LSR-ID for the LDP protocol is still valid and is the operationally UP IP address on an enabled loopback interface.

When you enter the **no** form of the command and LDP protocol is in the disabled state (this happens when the loopback interface on which IP address is configured is in the disabled state), the device falls back to default behavior which tries to enable LDP protocol when it finds a valid IP address on any one of the enabled loopback interfaces.

Examples

The following example configures an IP address for the LSR identifier.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# lsr-id 10.22.22.22
```

History

Release	Command history
5.5.00	This command is introduced.

mac access-group

Applies rules specified in a named or numbered MAC access control list (ACL) to traffic entering or exiting an interface.

Syntax

mac access-group { *acl-num* | *acl-name* } { **in** | **out** }

no mac access-group { *acl-num* | *acl-name* } { **in** | **out** }

Command Default

ACLs are not applied to interfaces.

Parameters

acl-num

Specifies an ACL number from 400 through 1399.

acl-name

Specifies an ACL name of up to 255 alphanumeric characters. The first character must be alphabetic.

in

Applies the ACL to inbound traffic on the port.

out

Applies the ACL to outbound traffic on the port.

Modes

Interface subtype configuration modes

Usage Guidelines

To apply a MAC ACL name that contains spaces, enclose the name in quotation marks (for example, **mac access-group "Deny-all ACL" in**).

To remove an ACL from an interface, use the **no** form of this command.

Examples

The following example creates a named MAC ACL, defines rules within, and then applies it to an interface.

```
device(config)# mac access-list example_l2_acl
device(config-mac-nacl)# deny 0000.0000.0001 ffff.ffff.ffff any
device(config-mac-nacl)# permit any 0000.0000.0002 ffff.ffff.ffff
device(config-mac-nacl)# exit
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2) #mac access-group example_l2_acl in
```

The first phase of the following example creates a numbered MAC ACL, containing rules that deny all ARP, IPv6, and MPLS multicast traffic; and permit all other traffic in VLAN 100.

```
device# configure terminal
device(config)# access-list 400 deny any any any etype arp
device(config)# access-list 400 deny any any any etype ipv6
device(config)# access-list 400 deny any any any etype 8848
device(config)# access-list 400 permit any any 100
```

The second phase of the example applies the ACL to a physical interface, to filter outbound traffic:

```
device(config)# interface ethernet 4/12
device(config-int-e100-4/12)# mac access-group 400 out
```

mac access-group enable-deny-logging

Running this command on an interface is one of the conditions for enabling logging of traffic denied by MAC ACLs applied to the interface. The other condition is the inclusion of the **log** parameter in rules within such ACLs.

Syntax

mac access-group enable-deny-logging [**hw-drop**]

no mac access-group enable-deny-logging [**hw-drop**]

Command Default

Deny-logging for MAC ACLs is disabled.

Parameters

hw-drop

Specifies that MAC ACL-log packets be dropped in hardware, which reduces CPU load.

Modes

Interface subtype configuration modes

Usage Guidelines

Deny-logging is supported for inbound ACLs only.

When this command is implemented with the **hw-drop** option, packet-counts of denied traffic will include only the first packet in each time cycle.

To disable MAC ACL deny-logging on an interface, use the **no mac access-group enable-deny-logging** command. You do not have to remove **log** parameters from ACLs and re-apply the ACLs.

To disable the **hw-drop** option, use the **no mac access-group enable-deny-logging hw-drop** command.

Examples

The following example implements MAC ACL deny-logging on an interface—for applied ACLs that contain rules with **log** parameters.

```
device# configure terminal
device(config)# interface ethernet 5/1
device(config-if-e1000-5/1)# mac access-group enable-deny-logging
```

mac access-list

Creates a named MAC access list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

mac access-list *acl-name*

no mac access-list *acl-name*

Command Default

No named MAC ACLs are defined.

Parameters

acl-name

Specifies a unique MAC ACL name. The name can be up to 255 characters, and must begin with an alphabetic character. If the name contains spaces, put it within quotation marks. Otherwise, no special characters are allowed, except for underscores and hyphens.

Modes

Global configuration mode

Usage Guidelines

After you create a named ACL, enter one or more [**sequence**] { **permit** | **deny** } commands to create filtering rules for that ACL.

You can create up to 500 named MAC ACLs.

A MAC ACL starts functioning only after if is applied to an interface using the **mac access-group** command.

You can create numbered MAC ACLs, using the **access-list** command.

The system supports the following MAC ACL resources:

- Numbered MAC ACLs—1000
- Named MAC ACLs—500
- Maximum filter-rules per MAC ACL—64. You can change the maximum up to 256 by using the **system-max l2-acl-table-entries** command.

The **no** form of this command deletes the ACL. You can delete a MAC ACL only after you first remove it from all interfaces to which it is applied, using the **no mac access-group** command.

Examples

The following example creates a named MAC ACL, defines rules within, and then applies it to an interface.

```
device(config)#mac access-list example_l2_acl
device(config-mac-nacl)#deny 0000.0000.0001 ffff.ffff.ffff any
device(config-mac-nacl)#permit any 0000.0000.0002 ffff.ffff.ffff
device(config-mac-nacl)#exit
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2)#mac access-group example_l2_acl in
```

mac-age-time

Tunes the system so it can function the most effectively based on the deployment and a specific configuration.

Syntax

mac-age-time [*dec* | **vpls** [**local** | **remote**]]

Parameters

dec

Sets the aging period, in seconds, to age the software MAC table.

vpls

Sets the aging period for VPLS mac entries.

local

MAC entries learned from local endpoints.

remote

MAC entries learned from PW.

Modes

Global configuration mode.

Usage Guidelines

- The values are bound by the same global system range shared with the regular MAC entries.
- The default values remain the same, which are 300 seconds for VPLS local entries and 600 seconds for the remote entries.
- Age time "0" disables the software aging. VPLS MAC follows the same format to be consistent. However, the value "0" is hidden as the valid range.
- When the software aging is disabled after the hardware aging is kicked in, and the software aging has already started, the age field displays the time value that elapsed prior to the aging being disabled.
- When the aging is re-enabled after a disable, the software aging resumes from the age value where it was stopped.
- Under the node *vpls*, you can specify a separate timer value for the local and the remote timers.
- The VPLS age timers are fully configurable for both local and remote entries.
- The formula '2 x' between the local timer and the remote timer is removed. Now, you have the flexibility to specify values for the age timers independently for the local and the remote entries.

Examples

The following example displays a sample configuration for the **mac-age-time** command:

```
device(config)# mac-age-time vpls remote 240
```

History

Release	Command history
5.5.00	This command is introduced.

mac-move-det-syslog

Enables the display of MAC movement syslog messages.

Syntax

mac-move-det-syslog

no mac-move-det-syslog

Command Default

By default, MAC movement syslog messages are displayed.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the display of MAC movement syslog messages.

NOTE
This command is only supported on Brocade NetIron MLX Series devices.

Examples

The following example shows the MAC movement syslog message output when **mac-move-det-syslog** command is used.

```
device(config)# mac-move-det-syslog
device(config)# show arp

Total number of ARP entries: 2
(In all VRFs)

Entries in default routing instance:
IP  Address       MAC Address     Type     Age Port (Vpls-Id, Vlan)/ Vpls-Id:Peer

1   10.19.19.1    0010.9400.0606  Dynamic  1   1/24
2   172.26.67.1   0024.381c.b900  Dynamic  1   mgmt1
device(config)# exit
device#
SYSLOG: <12>Sep 25 02:43:07 IP/ARP: IP address 19.19.19.1 MAC movement detected,
        changed from MAC 0010.9400.0606 / port 1/24 to MAC 0010.9400.0001 / port 1/24

device#
device#
device# configure terminal
device(config)# show arp
Total number of ARP entries: 2
(In all VRFs)

Entries in default routing instance:
IP  Address       MAC Address     Type     Age Port (Vpls-Id, Vlan)/ Vpls-Id:Peer

1   10.19.19.1    0010.9400.0001  Dynamic  1   1/24
2   172.26.67.1   0024.381c.b900  Dynamic  2   mgmt1
device(config)#
device(config)#
SYSLOG: <12>Sep 25 02:43:40 IP/ARP: IP address 19.19.19.1 MAC movement detected,
        changed from MAC 0010.9400.0001 / port 1/24 to MAC 0010.9400.0606 / port 1/24
```

The following example shows the MAC movement syslog message output when the display is disabled.

```
device(config)#no mac-move-det-syslog
device(config)#
device(config)# exit
device# show arp
Total number of ARP entries: 2
(In all VRFs)

Entries in default routing instance:
IP  Address       MAC Address     Type     Age Port (Vpls-Id, Vlan)/ Vpls-Id:Peer

1   10.19.19.1    0010.9400.0001  Dynamic  1   1/24
2   172.26.67.1   0024.381c.b900  Dynamic  2   mgmt1
device#
device#
```

History

Release version	Command history
5.7.00	This command was introduced.

macsec cipher-suite

Enables GCM-AES-128 bit encryption or GCM-AES-128 bit integrity checks on MACsec frames transmitted between group members.

Syntax

macsec cipher-suite gcm-aes-128 [**integrity-only**]

no macsec cipher-suite gcm-aes-128 [**integrity-only**]

Command Default

By default GCM-AES-128 bit encryption or integrity checking is not enabled. Frames are encrypted starting with the first byte of the data packet, and ICV checking is enabled.

Parameters

gcm-aes-128
Enables GCM-AES-128 bit encryption.

integrity-only
Enables GCM-AES-128 bit integrity checks.

Modes

dot1x-mka-cfg-group mode.

Usage Guidelines

The **macsec cipher-suite** command can be used in conjunction with an encryption offset configured using the **macsec confidentiality-offset** command.

The no form of the command restores the default encryption and integrity checking.

NOTE

- When cipher suite is configured without integrity the capability of the system is confidentiality and integrity plus confidentiality offset 0.
- When integrity only is configured, then confidentiality offset configuration is not allowed and vice-versa.

Examples

The following example enables GCM-AES-128 encryption for group1.

```
device# configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec cipher-suite gcm-aes-128
```

The following example enables GCM-AES-128 bit integrity checking for group1.

```
device# configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec cipher-suite gcm-aes-128 integrity-only
```

History

Release version	Command history
5.8.00	This command was introduced.

macsec confidentiality-offset

Configures the offset size for MACsec encryption.

Syntax

macsec confidentiality-offset *size*

no macsec confidentiality-offset *size*

Command Default

By default the offset size is set to 0.

Parameters

size

Specifies the off-set value of 0 bytes. Valid values are:

0
: Complete packet is encrypted.

30
: Encryption begins at byte 31 of the data packet.

50
: Encryption begins at byte 51 of the data packet.

Modes

dot1x-mka-cfg-group mode

Usage Guidelines

The **no** form of the command disables encryption offset on all interfaces in the MACsec MKA group.

This command is applicable only when encryption is enabled for the MACsec group using the **macsec cipher-suite** command.

NOTE
Configuring the confidentiality off-set value to 0 bytes is not allowed.

Examples

The following example configures a 30-byte offset on encrypted transmissions as part of the parameters for group1.

```
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec confidentiality-offset 30
```

History

Release version	Command history
5.8.00	This command was introduced.

macsec frame-validation

Enables validation checks for frames with MACsec headers and configures the validation mode (strict or not strict).

Syntax

macsec frame-validation [**disable** | **check** | **strict**]

no macsec frame-validation [**disable** | **check** | **strict**]

Command Default

By default **strict** parameter is set as frame-validation mode.

Parameters

disable

Disables validation checks for frames with MACsec headers.

check

Enables validation checks for frames with MACsec headers and configures non-strict validation mode. If frame validation fails, counters are incremented but packets are accepted.

strict

Enables validation checks for frames with MACsec headers and configures strict validation mode. If frame validation fails, counters are incremented and packets are dropped.

Modes

dot1x-mka-cfg-group mode.

Usage Guidelines

The **no** form of the command restores the default mode of validation, (validation checks for frames with MACsec headers is disabled).

Examples

The following example enables validation checks for frames with MACsec headers on group group1 and configures strict validation mode.

```
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec frame-validation check
```

History

Release version	Command history
5.8.00	This command was introduced.

macsec replay-protection

Specifies the action to be taken when packets are received out of order, based on their packet number. If replay protection is configured, you can specify the window size within which out-of-order packets are allowed.

Syntax

macsec replay-protection [**strict** | **out-of-order window-size** *size*]

no macsec replay-protection [**strict** | **out-of-order window-size** *size*]

Command Default

Macsec replay protection is enabled in Strict mode.

Parameters

strict

Does not allow out-of-order packets.

out-of-order window size *size*

Specifies the allowable window within which an out-of-order packet can be received. Allowable range is from 1 through 4294967295.

Modes

dot1x-mka-cfg-group mode

Usage Guidelines

The **no** form of the command disables macsec replay protection.

Examples

The following example configures group group1 to accept packets with window size 100.

```
device# configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec replay-protection out-of-order window-size 100
```

History

Release version	Command history
5.8.00	This command was introduced.

match additional paths advertise-set

Matches the additional BGP paths that are candidates to be advertised in a route map instance.

Syntax

match additional paths advertise-set { **all** | **best** *number* | **best-range** *start-range end-range* | **group-best** }

no match additional paths advertise-set { **all** | **best** *number* | **best-range** *start-range end-range* | **group-best** }

Command Default

Paths are not matched.

Parameters

all

Specifies all paths.

best

Specifies the paths that the device selects as best paths.

number

Specifies the number of best paths. Valid values range from 2 through 16.

best-range *start-range end-range*

Specifies a range of best paths. Valid values range from 1 through 16.

group-best

Specifies the group best paths.

Modes

Route map configuration mode

Usage Guidelines

This command can only be configured once in any route map instance. Once it is used in a route map instance, any subsequent use overwrites the existing configuration.

The **no** form of the command removes the BGP additional paths match statement from the route map instance.

Examples

The following example matches the nine best BGP paths as additional BGP paths that are candidates to be advertised.

```
device# configure terminal
device(config)# route-map myroutemap permit 1
device(config-routemap myroutemap)# match additional paths advertise-set 9
```

History

Release version	Command history
6.0.0	The command was introduced.

match identity

Configures the selection of IKEv2 profile Peer Authorization Database (PAD) for a peer based on local or remote identity parameters received.

Syntax

match identity {**local** {**address** *ip address* | **dn** *dn name* | **email** *email address* | **fqdn** *fqdn name* | **key-id** *key ID name* } **| remote** {**address** *ip address* | **dn** *dn name* | **email** *email address* | **fqdn** *fqdn name* | **key-id** *key ID name* } }

no match identity {**local** {**address** *ip address* | **dn** *dn name* | **email** *email address* | **fqdn** *fqdn name* | **key-id** *key ID name* } **|** **remote** {**address** *ip address* | **dn** *dn name* | **email** *email address* | **fqdn** *fqdn name* | **key-id** *key ID name* } }

Parameters

ipv4 address
Specifies the local IP address in the identity parameter received.

dn name
Specifies the DN value.

email address
Specifies the email address.

fqdn name
Specifies the FQDN name.

key id name
Specifies the key ID name.

ipv4 address
Specifies the remote IP address in the identity parameter received.

dn name
Specifies the DN name for the remote identity parameter received.

email address
Specifies the email address for the remote identity parameter received.

fqdn name
Specifies the FQDN name for the remote identity parameter received.

key id name
Specifies the key ID name for the remote identity parameter received.

Modes

IKEv2 profile configuration mode

Usage Guidelines

no

Examples

The following example configures the selection of IKEv2 profile (PAD) for a peer based on local IPv4 address.

```
device(config)# ikev2 profile brocade
device(config-ikev2-profile-brocade)# match identity local address 10.20.20.10
```

History

Release version	Command history
05.8.00	This command was introduced.

match l2acl

Configures a route map that matches with the configured Layer 2 ACL.

Syntax

match l2acl { *acl-number* | *acl-name* }

no match l2acl { *acl-number* | *acl-name* }

Command Default

The Layer 2 ACL information is not configured in the route map configuration.

Parameters

acl-number

Specifies the numbered Layer 2 ACL.

acl-name

Specifies the named Layer 2 ACL.

Modes

Route map configuration mode .

Usage Guidelines

Five Layer 2 ACLs separated by spaces can be added in the **match l2acl** configuration of the route map.

The **no** form of the command removes the Layer 2 ACL match statement from the route map.

Examples

The following example configures a route map that matches with the configured Layer 2 ACL.

```
device(config)# route-map xGW_map permit 1
device(config-routemap xGW_map)# match l2acl abc
```

The following example configures multiple Layer 2 ACLs to a route map.

```
device(config)# route-map xGW_map permit 1
device(config-routemap xGW_map)# match l2acl 400 401 402
```

History

Release version	Command history
5.8.00b	The command was introduced.

maximum-paths (IS-IS)

Specifies the number of paths IS-IS can calculate and install in the IP or IPv6 forwarding table.

Syntax

maximum-paths *number*

no maximum-paths *number*

Command Default

The default is 4.

Parameters

value

Specifies the number of paths. Valid values range from 1 through 8. The default is 4.

Modes

ISIS address-family IPv4 unicast configuration mode

ISIS address-family IPv6 unicast configuration mode

Usage Guidelines

The maximum number of paths supported by the BR-MLX-10Gx24-DM module is 16.

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

Examples

The following example specifies that the number of paths IS-IS can calculate and install in the IP forwarding table is 5.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-isis-router-ipv4u)# maximum-paths 5
```

The following example restores the default so that the number of paths IS-IS can calculate and install in the IPv6 forwarding table is 4.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-isis-router-ipv6u)# no maximum-paths
```

max-lsp-lifetime

Sets the maximum number of seconds an unrefreshed Link State PDU (LSP) remains in the LSP database of a device.

Syntax

max-lsp-lifetime *secs*

max-lsp-lifetime *secs*

Command Default

The default maximum lifetime is 1200 seconds (20 minutes).

Parameters

secs

Specifies the maximum lifetime in seconds. Valid values range from 1 through 65535 seconds. The default is 1200 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

The **max-lsp-lifetime** and **lsp-refresh-interval** commands must be configured in such a way that the LSPs are refreshed before the maximum LSP lifetime is reached; otherwise, the device's originated LSPs may be timed out by neighbors of the device.

The **no** form of the command removes the configured period of time.

Examples

The following example changes the maximum LSP lifetime to 2400 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# max-lsp-lifetime 2400
```

max-metric router-lsa (OSPFv2)

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Syntax

max-metric router-lsa [**all-lsas**] [**all-vrfs**] [**external-lsa** *metric-value*] [**link** { **all** | **ptp** | **stub** | **transit** }] [**on-startup** { *time* | **wait-for-bgp** }] [**summary-lsa** *metric-value*] [**te-lsa** *metric-value*]

no max-metric router-lsa [**all-lsas**] [**all-vrfs**] [**external-lsa** *metric-value*] [**link** { **all** | **ptp** | **stub** | **transit** }] [**on-startup** { *time* | **wait-for-bgp** }] [**summary-lsa** *metric-value*] [**te-lsa** *metric-value*]

Parameters

all-lsas

Sets the **external-lsa**, **summary-lsa**, and **te-lsa** optional parameters to the corresponding default max-metric value.

all-vrfs

Applies the configuration change to all instances of OSPFv2.

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 through 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.

on-startup

Specifies the advertisement of the maximum metric for a limited period only, on 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 through 86400.

wait-for-bgp

Specifies that the maximum metric is advertised until BGP converges, or for 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 through 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

te-lsa *metric-value*

Specifies that the TE metric field in the TE metric sub tlv for all type 10 Opaque LSAs LINK TLV originated by the router will be modified to the specified metric-value or a default value. The range for metric-value are 1 through 4294967295 (Hex: 0x00001 to 0xFFFFFFFF). The default value is 4294967295 (Hex: 0xFFFFFFFF). This parameter only applies to the default instance of OSPF.

Modes

OSPFv2 router configuration mode

OSPFv2 router VRF configuration mode

Usage Guidelines

Use this command to enable OSPFv2 to advertise its locally generated router LSAs with a maximum metric to direct transit traffic away from the device, while still routing for directly connected networks. By advertising the maximum metric, the device does not attract transit traffic.

Any new OSPFv2 instance configured after the max-metric configuration is completed requires that the **max-metric** command be configured again to take in the new OSPFv2 instance.

The **no** form of the command disables the advertising of the maximum metric value in different LSAs.

Examples

The following example turns off the advertisement of special metric values in all router, summary, and external LSAs.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# no max-metric router-lsa
```

The following example configures an OSPFv2 device to advertise a maximum metric for 72 seconds after a restart before advertising with a normal metric.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# max-metric router-lsa on-startup 72
```

The following example indicates that OSPF is being shutdown and that all links in the router LSA should be advertised with the value 0xFFFF and the metric value for all external and summary LSAs is set to 0xFF0000 until OSPF is restarted. This configuration will not be saved.

```
device# configure terminal
device(config)# ip router ospf
device(config-ospf-router)# max-metric router-lsa external-lsa summary-lsa link all
```

max-metric router-lsa (OSPFv3)

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Syntax

max-metric router-lsa [**external-lsa** *metric-value* | **include-stub** | **on-startup** { *time* | **wait-for-bgp** } | **summary-lsa** *metric-value*]

no max-metric router-lsa [**external-lsa** | **include-stub** | **on-startup** { *time* | **wait-for-bgp** } | **summary-lsa**]

Parameters

external-lsa *metric-value*

Configures the maximum metric value for all external type-5 and type-7 LSAs. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

include-stub

Specifies the advertisement of the maximum metric value for point-to-point and broadcast stub links in the intra-area-prefix LSA..

on-startup

Applies the configuration change at the next OSPF startup.

time

Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86400.

wait-for-bgp

Specifies that OSPFv3 should wait until BGP has finished route table convergence before advertising the links with the normal metric, or for no more than 600 seconds.

summary-lsa *metric-value*

Configures the maximum metric value for all summary type 3 and type 4 LSAs. The range for metric value is 1 to 16777215 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Enter **no max-metric router-lsa** to disable advertising the maximum metric value in different LSAs.

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.

- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

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-ospf6-router)# 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-ospf6-router)# max-metric router-lsa include-stub
```

The following example configures an OSPFv3 device to advertise a maximum metric for 75 seconds after a restart before advertising with a normal metric.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# max-metric router-lsa on-startup 75
```

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-ospf6-router)# 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-ospf6-router)# max-metric router-lsa summary-lsa 100
```

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

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

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.

Examples

This example configures the device to favor a route containing a MED.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# med-missing-as-worst
```

method

Configures the IKEv2 authentication method.

Syntax

method {**local {ecdsa384 | pre-shared}** | **remote {ecdsa384 | pre-shared}** }

no method {**local {ecdsa384 | pre-shared}** | **remote {ecdsa384 | pre-shared}** }

Parameters

local

Specifies the local authentication method.

remote

Specifies the remote authentication method.

ecdsa384

Specifies the digital signature for the authentication certificate.

pre-shared

Specifies the pre-shared key value.

Modes

IKEv2 auth-proposal configuration mode

Usage Guidelines

no

Examples

The following example configures IKEv2 authentication method.

```
device(config)# ikev2 auth-proposal brocade
device(config-ike-auth-brocade)# method local ecdsa384
```

History

Release version	Command history
05.8.00	This command was introduced.

metric

Assigns a metric to the LSP, which routing protocols can use to determine the relative preference among several LSPs towards a given destination.

Syntax

metric *number*

no metric *number*

Command Default

All LSPs have a metric of 1.

Parameters

number

Specifies the metric value. Enter an integer from 1 to 65535. A lower value is preferred over a higher value.

Modes

MPLS LSP configuration mode

Usage Guidelines

When multiple LSPs have the same destination LSR, and they have the same metric, the traffic load is shared among them.

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

Examples

The following example configures LSP to22 with a metric value of 20.

```
device(config)# router mpls
device(config-mpls)# lsp to22
device(config-mpls-lsp-to22)# disable
Disconnecting signaled LSP to22
device(config-mpls-lsp-to22)# to 10.1.1.2
device(config-mpls-lsp-to22)# from 10.1.1.1
device(config-mpls-lsp-to22)# metric 20
device(config-mpls-lsp-to22)# enable
Connecting signaled LSP to22
```

metric-style wide

Enables the wide metric type for new style of TLVs with Intermediate System-to-Intermediate System (IS-IS).

Syntax

metric-style wide [**level-1** | **level-2**]

no metric-style wide

Command Default

The wide metric type is not used.

Parameters

level-1

Specifies the IS-IS routing parameter as Level 1.

level-2

Specifies the IS-IS routing parameter as Level 2.

Modes

IS-IS address-family IPv4 unicast configuration mode

Usage Guidelines

If the IS-IS routing parameter is not configured, the metric value is applied to both Level 1 and Level 2 packets.

When LDP-IGP synchronization is enabled, the wide metric type must be used.

The **no** form of the command disables the use of the wide metric type.

Examples

The following example enables the wide metric type for Level 1 packets for the IS-IS IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-isis-router-ipv4u)# metric-style wide level-1
```

metric-type

Configures the default metric type for external routes.

Syntax

metric-type { **type1** | **type2** }

no metric-type { **type1** | **type2** }

Command Default

Type 2

Parameters

type1

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

type2

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

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default setting. You must specify a type parameter when using the **no** form.

Examples

The following example sets the default metric type for external routes to type 1.

```
device# configure terminal
device(config)# router ospf
device(config-ospf6-router)# metric-type type1
```

The following example sets the default metric type for external routes to type 2.

metro-ring

Adds a metro ring to a port-based VLAN and enters MRP configuration mode.

Syntax

metro-ring *ring-id*

no metro-ring *ring-id*

Command Default

A metro ring is not added to a port-based VLAN.

Parameters

ring-id

Specifies the ID of the metro ring. The ring ID ranges from 1 through 255.

Modes

VLAN configuration mode

Usage Guidelines

If you plan to use a topology group to add VLANs to the ring, make sure you configure MRP on the topology group master VLAN.

If you want to add more than one metro ring to a port-based VLAN, use the **metro-rings** command.

The **no** form of the command removes the metro ring from the port-based VLAN.

Examples

The following example shows how to add the metro ring to a port-based VLAN.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)#
```

mka-auth-fail-action

Configures MACsec Key Agreement (MKA) authentication fail action on MKA group.

Syntax

mka-auth-fail-action [**allow-unencrypted-traffic** | **deny-all-traffic**]

no mka-auth-fail-action [**allow-unencrypted-traffic** | **deny-all-traffic**]

Command Default

By default, **deny-all-traffic** is enabled.

Parameters

allow-unencrypted-traffic

Allows unencrypted traffic exchange between peers, even if MKA authentication fails.

deny-all-traffic

Drops all traffic exchange between peers, if MKA authentication fails.

Modes

MKA group configuration mode.

Usage Guidelines

The key-server is elected by comparing key-server priority values during MKA message exchange between peer devices, in-case no peer is elected as key server then the MKA protocol moves to failed state. Under such scenario default behavior is to drop all the traffic on the link. However this behavior can be controlled using **mka-auth-fail-action** command by allowing unencrypted traffic exchange between peer devices even if MKA protocol fails.

The **no** form of the command disables MKA authentication fail action configuration on MKA group.

Examples

The following example explains how to configure MKA authentication fail action on MKA group.

```
device(config)#dot1x-mka-enable
device(config-dot1x-mka)#mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)#mka-auth-fail-action allow-unencrypted-traffic
```

History

Release version	Command history
5.8.00	This command was introduced.

mka-cfg-group

Configures a MACsec Key Agreement (MKA) configuration groups and enabling this command will enter into mka-cfg-group mode .

Syntax

mka-cfg-group *group-name*

no mka-cfg-group *group-name*

Parameters

group-name

Specifies the MKA configuration group name that can be applied to ports.

Modes

dot1x-mka configuration mode.

Usage Guidelines

The **dot1x-mka-enable** command must be executed before the **mka-cfg-group** command can be used.

NOTE

1. When a group is created, all group parameters will be assigned with the default values.
2. Maximum number of groups allowed is 128.

The **no** form of this command deletes the MKA configuration group.

Examples

The following example configures the MKA configuration group, group1.

```
device(config-dot1x-mka)# mka-cfg-group  group1
device(config-dot1x-mka-cfg-group-group1)#
```

History

Release version	Command history
5.8.00	This command was introduced.

mmrp enable

Enables MMRP..

Syntax

mmrp enable

no mmrp enable

Command Default

MMRP is disabled.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

Using the command at the interface level enables MMRP on that interface. To configure MMRP at the interface level, MMRP must be enabled at global level first.

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

Examples

The following example enables MMRP globally.

```
device(config)# mmrp enable
```

The following example enables MMRP at the interface.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mmrp enable
```

mmrp include-vlan

Configures a set of VLANs on which MMRP is allowed to participate.

Syntax

mmrp include-vlan *vlan-id* [**to** *vlan-id*]

no mmrp include-vlan *vlan-id* [**to** *vlan-id*]

Command Default

By default, no VLANs are allowed to participate in MMRP.

Parameters

vlan-id

Specifies the VLAN ID.

to

Specifies a range of VLAN.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The global configuration is applicable to all the MMRP enabled ports unless an explicit configuration is made on the port. Only 256 B-VLANs are allowed to participate in MMRP.

The interface VLANs are allowed only when they are configured under global **mmrp include-vlan** command.

On Brocade NetIron CER Series and Brocade NetIron CES Series devices, the VLAN should be in theB-VLAN ESI. On Brocade NetIron MLX Series and Brocade NetIron XMR Series devices, the B-VLAN must be alayer 2 (L2) VLAN.

The **no** form of the command removes the VLANs.

Examples

The following example configures a set of VLANs on which MMRP is allowed to participate.

```
device(config)# mmrp include-vlan 100
```

The following example configures a set of VLANs on an interface on which MMRP is allowed to participate.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mmrp include-vlan 100 to 200
```

mmrp point-to-point

Configures an interface as point-to-point for MMRP.

Syntax

mmrp point-to-point

no mmrp point-to-point

Command Default

By default, point-to-point is disabled.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables point-to-point.

Examples

The following example configures a single interface as point-to-point.

```
device(config)# interface ethernet 1/1
device(config-eth-1/1)# mmrp enable
device(config-eth-1/1)# mmrp include-vlan 300
device(config-eth-1/1)# mmrp include-vlan 1000 1100
device(config-eth-1/1)# mmrp timer join 400 leave 1200 leave-all 10000
device(config-eth-1/1)# mmrp point-to-point
```

The following example configures multiple consecutive interface as point-to-point.

```
device(config)# interface ethernet 1/1 to ethernet 1/2
device(config-mif-1/1-1/2)# mmrp enable
device(config-mif-1/1-1/2)# mmrp include-vlan 300
device(config-mif-1/1-1/2)# mmrp include-vlan 1000 1100
device(config-mif-1/1-1/2)# mmrp timer join 400 leave 1400 leave-all 10000
device(config-mif-1/1-1/2)# mmrp point-to-point
```

The following example configures multiple non-consecutive interface as point-to-point.

```
device(config)# interface ethernet 1/1 ethernet 1/3 ethernet 1/5
device(config-mif-1/1,1/3,1/5)# mmrp enable
device(config-mif-1/1,1/3,1/5)# mmrp include-vlan 300
device(config-mif-1/1,1/3,1/5)# mmrp include-vlan 1000, 1100
device(config-mif-1/1,1/3,1/5)# mmrp timer join 400 leave 1400 leave-all 10000
device(config-mif-1/1,1/3,1/5)# mmrp point-to-point
```

mmrp registration-mode

Configures the registration mode for MACs to be forbidden.

Syntax

mmrp registration-mode forbidden vlan *vlan-id* **mac-address** *mac-address-vlaue* [**to** *mac-address-vlaue*]

mmrp registration-mode forbidden vlan *vlan-id* **mac-address** *mac-address-vlaue* [**to** *mac-address-vlaue*]

Command Default

By default, registration mode for a MAC attribute is normal.

Parameters

forbidden
Blocks the dynamic registration of these attributes.

vlan *vlan-id*
Specifies the VLAN ID.

mac-address *mac-address-value*
Specifies the MAC address.

to *mac-address-value*
Specifies a range for the MAC address.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command removes the forbidden registration mode for MACs.

Examples

The following example configures the registration mode for MACs to be forbidden.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mmrp registration-mode forbidden 011E.8300.3001
```

mmrp timer

Configures the join, leave, and leave-all timers for MMRP.

Syntax

mmrp timer join *join-timer* **leave** *leave-timer* **leave-all** *leave-all-timer*

no mmrp timer join *join-timer* **leave** *leave-timer* **leave-all** *leave-all-timer*

Command Default

The default value for the Join timer is 200 ms, the default value for the leave timer is 1000ms, and the default value for the leave-all timer is 10000ms.

Parameters

join *join-timer*

Configures the join timer. The range is from 200 to 100000000ms.

leave *leave-timer*

Configures the leave timer. The range is from 1000 to100000000ms.

leave-all timer

Configures the leave-all timer. The range is from 10000 to 100000000ms.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The Leave timer should be greater than or equal to twice the join timer plus 600ms. Leave-all timer should be large relative to the Leave timer; recommended value is at least three times the value of Leave timer.

The **no** form of the command rests the timers to the default value.

Examples

The following example configures the MMRP timers at the global level.

```
device(config)# mmrp timer join 400 leave 1400 leave-all 10000
```

The following example configures MMRP timer on an interface.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mmrp timer join 400 leave 1400 leave-all 10000
```

mpls-interface

Configures MPLS on an interface and accesses MPLS interface sub-configuration mode to configure its parameters.

Syntax

mpls-interface { **ethernet** *slot/port* | **ve** *number*}

no mpls-interface { **ethernet** *slot/port* | **ve** *number*}

Command Default

None

Parameters

ethernet *slot/port*

Specifies an Ethernet slot and port.

ve *number*

Specifies the VE interface number.

Modes

MPLS configuration mode

Usage Guidelines

Use the **no** form of this command to remove the MPLS interface.

You cannot configure MPLS on a VE interface associated with a protocol based VLAN. The command is rejected, and an error message is displayed.

After you enable MPLS globally on the device, you can enable it on one or more interfaces.

Examples

The following example configures MPLS on Ethernet interface 1/12.

```
device(config)# router mpls
device(config-mpls)# mpls-interface ethernet 1/12
device(config-mpls-if-e-1/12)#
```

multi-topology

Enables IPv6 Intermediate System-to-Intermediate System (IS-IS) MT in an area or a domain so that the MT-enabled device runs IPv6 IS-IS in multi SPF mode.

Syntax

multi-topology [**transition**]

no multi-topology [**transition**]

Command Default

The transition option is disabled.

Parameters

transition

Enables IPv6 IS-IS MT transition mode in an area or a domain so that a network operating in IPv6 IS-IS single-topology support mode can continue to work while upgrading devices to include IPv6 IS-IS MT support.

Modes

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

When transition mode is not enabled, the routers operating in single-topology mode do not establish IPv6 connectivity with the routers operating in MT mode.

The **no** form of the command disables IPv6 IS-IS MT.

Examples

The following example enables IPv6 IS-IS MT.

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

The following example enables IPv6 IS-IS MT with transition support.

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

mvrp applicant-mode

Configures applicant-mode for MVRP.

Syntax

mvrp applicant-mode { **non-participant** | **normal-participant** }

no mvrp applicant-mode { **non-participant** | **normal-participant** }

Command Default

Applicant mode by default is set as normal participant.

Parameters

non-participant

Configure MVRP applicant mode as non-participant so that PDUs are not transmit PDUs on this port; and therefore, no VLAN declarations are made.

normal-participant

Configure MVRP applicant mode as normal participant so that PDUs are transmitted on this port for making VLAN declarations.

Modes

Interface configuration mode

Usage Guidelines

The applicant mode must be configured as non-participant over a port should be used for edge port.

The **no** form of the command rests the applicant mode as normal-participant.

Examples

The following example configures MVRP applicant mode as non-participant.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mvrp applicant-mode non-participant
```

mvrp enable

Enables MVRP.

Syntax

mvrp enable

no mvrp enable

Command Default

MVRP is disabled.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

MVRP must be enabled globally to allow the device to participate in the protocol.

After enabling MVRP at the global level, MVRP must be enabled on the required interfaces. Use the command from the interface configuration mode to enable MVRP on an interface. Before MVRP can be configured at the interface level, it must be enabled at global level first.

Use the **no** form of the command to disable MVRP.

Examples

The following example enables MVRP.

```
device(config)# mvrp enable
```

The following example enables MVRP on the interface Ethernet 1/1.

```
device(config)# mvrp enable
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mvrp enable
```

mvrp point-to-point

Configures MVRP point-to-point over a port.

Syntax

mvrp point-to-point

no mvrp point-to-point

Command Default

By default, point-to-point is disabled.

Modes

Interface configuration mode

Usage Guidelines

Configuring point to point over a port should be used when a port is connected to a shared media device.

The no form of the command disables point-to-point.

Examples

The following example configures MVRP point-to-point over a port.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mvrp point-to-point
```

mvrp registration-mode forbidden

Configures the MVRP registration mode as forbidden.

Syntax

mvrp registration-mode forbidden vlan *vla-id*[**to** *vlan-id*]

no mvrp registration-mode forbidden vlan *vla-id*[**to** *vlan-id*]

Command Default

By default, registration mode is normal.

Parameters

vlan *vlan-id*

Specifies the VLAN ID.

to *vlan-id*

Specifies a range of VLAN IDs.

Modes

Interface configuration mode

Usage Guidelines

Configure this command to block the dynamic registration of MVRP attributes.

For a static VLAN configuration, registration mode is automatically set to Fixed.

The **no** form of the command resets the registration mode to normal.

Examples

The following example configures the MVRP registration mode as forbidden.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mvrp registration-mode forbidden vlan 10
```

mvrp timer

Configures the join, leave and leave-all timers at global level for MVRP.

Syntax

mvrp timer join *join-timer* **leave** *leave-timer* **leave-all** *leaveall-timer*

no mvrp timer join *join-timer* **leave** *leave-timer* **leave-all** *leaveall-timer*

Command Default

The default values are: Join timer - 200ms; Leave timer - 1000ms; Leave-all timer - 10000m.

Parameters

join *join-timer*

Configures the MVRP join timer vlaue in milliseconds. Valid range is from 200 to 100000000 ms.

leave *leave-timer*

Configures the MVRP leave timer value in milliseconds. Valid range is from 1000 to 100000000 ms. The recommended value is 5000m.

leave-all *leaveall-timer*

Configures the MVRP leave-app timer value in milliseconds.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The leave timer must be greater than or equal to twice the join timer plus 600ms. The recommended value for the leave-all timer is at least three times the value of leave timer.

Use the command in interface configuration mode to configure the timers for a particular interface.

The **no** form of the command rests the timers to the default values.

Examples

The following example configures the MVRP timers at the global level.

```
device(config)# mvrp timer join 400 leave 1400 leave-all 10000
```

The following example configures the MVRP timer for the interface Ethernet 1/1

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# mvrp timer join 500 leave 1500 leave-all 15000
```

neighbor bfd

Enables Bidirectional Forwarding Detection (BFD) sessions for specified BGP neighbors or peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **bfd** { **holdover-interval** *time* | **min-tx** *transmit-time* **min-rx** *receive-time* **multiplier** *number* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **bfd** { **holdover-interval** *time* | **min-tx** *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.

min-tx *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 value is 1000 (unless changed at the global level).

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 value is 1000 (unless changed at the global level).

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

Usage Guidelines

Before using the **holdover-interval**, **min-tx**, **min-rx**, and **multiplier** parameters, you must first enable BFD.

When Brocade NetIron CER Series or Brocade NetIron CES Series devices are heavily loaded or under stress, BFD sessions may flap if the configured BFD interval is less than 500 milliseconds with a multiplier value of 3.

The **no** form of this command removes the BFD for BGP configuration for BGP neighbors or peer groups.

Examples

The following example sets the BFD holdover interval for a specified peer group to 18.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor pg1 bfd holdover-interval 18
```

The following example sets the BFD session timer values for a BGP neighbor with the IP address 10.1.1.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor 10.1.1.1 bfd min-tx 120 min-rx 150 multiplier 8
```

The following example sets the BFD session timer values for a BGP neighbor with the IP address 10.1.1.1 for VRF “red” in BGP address-family IPv4 unicast VRF configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 10.1.1.1 bfd min-tx 120 min-rx 150 multiplier 8
```

neighbor additional-paths

Enables additional paths capability for specified BGP neighbors.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths receive** [**send**]

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths send** [**receive**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths receive** [**send**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths send** [**receive**]

Command Default

Additional paths are not advertised.

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.

receive
: Enables BGP capability to receive additional paths from BGP neighbors.

send
: Enables BGP capability to send additional paths to BGP neighbors.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 multicast configuration mode

BGP address-family IPv6 multicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Capability configured at the peer level using this command overrides any send or receive capability configured at the address-family or peer-group level using the **additional-paths** command.

Examples

The following example enables BGP4 capability to send additional paths to a specified BGP neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.11.12.13 additional-paths send
```

The following example enables BGP4+ capability to receive additional paths from a specified BGP neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 additional-paths receive
```

History

Release version	Command history
6.0.0	This command was introduced.

neighbor additional-paths advertise

Applies filters for the advertisement of additional paths for BGP neighbors.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise all** [**best** *number*] [**group-best**]

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise best** *number* [**all**] [**group-best**]

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise group-best** [**all**] [**best** *number*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise** { **all** | **best** *number* | **group-best** }

Command Default

Filters are not 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.

all

Advertises all BGP additional paths with a unique next hop. The maximum number of paths is 16.

best

Advertises the additional paths that the device selects as best paths.

number

Specifies the number of best paths advertised. Valid values range from 2 through 16.

group-best

Specifies the group best paths. If the rank of any group-best add-path is more than 16, its is not advertised.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 multicast configuration mode

BGP address-family IPv6 multicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The set of paths to be advertised must be a subset of the selected paths configured using the **additional-paths select** command.

The **no** form of the command disables the configured filter.

Examples

The following example configures BGP4 to advertise all BGP additional paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.11.12.13 additional-paths advertise all
```

The following example configures BGP4+ advertise the four best BGP additional paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 additional-paths advertise best 4
```

History

Release version	Command history
6.0.0	This command was introduced.

neighbor additional-paths disable

Disables the advertisement of additional paths for specified BGP neighbors or peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **disable**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **disable**

Command Default

Disabled.

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 multicast configuration mode

BGP address-family IPv6 multicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

If the capability to send and receive additional paths is configured at the address family level using the **additional-paths** command, this capability is applied to all the neighbors under the address family. Use this command to disable this capability for a specified neighbor or peer group.

When additional-path capability is enabled at the peer-group or address-family level, this command can be used to disable the capability at the neighbor level. When additional-path capability is enabled at the address family level, this command can be used to disable the capability at the peer-group level.

Examples

The following example disables the sending of additional paths by BGP4 to a specified BGP neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.11.12.13 additional-paths disable
```

History

Release version	Command history
6.0.0	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**

Command Default

Disabled.

Parameters

ip-address
Specifies the IPv4 address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies a peer group.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 multicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

When this command is entered in BGP global configuration mode, it applies only to the IPv4 address family. Use this command in BGP address-family IPv6 unicast configuration mode for BGP4+ configurations. 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. When the **neighbor ebgp-btsh** command is used, BGP control packets sent by the device to a neighbor have a TTL value of 255. In addition, the device expects the BGP control packets received from the neighbor to have a TTL value of either 254 or 255. For multihop peers, 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. If the BGP control packets received from the neighbor do not have the anticipated value, the device drops them.

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)# 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)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 prefix-list ebgp-btsh
```

neighbor fail-over

Enables or disables Bidirectional Forwarding Detection (BFD) protocol support for failover.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **fail-over** { **bfd-enable** | **bfd-disable** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **fail-over** { **bfd-enable** | **bfd-disable** }

Command Default

BFD support for failover is disabled.

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.

bfd-enable
Enables BFD support for failover.

bfd-disable
Disables BFD support for failover.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command disables BFD support for failover.

Examples

The following example enables BFD support for failover for a BGP neighbor with the IP address 10.1.1.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor 10.1.1.1 fail-over bfd-enable
```

The following example enables BFD support for failover for a BGP neighbor with the IP address 10.1.1.1 for VRF instance "blue" in BGP address-family IPv4 unicast VRF configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf blue
device(config-bgp-ipv4u-vrf)# neighbor 10.1.1.1 fail-over bfd-enable
```

The following example enables BFD support for failover for a BGP peer group.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-ipv4u-vrf)# neighbor pg1 fail-over bfd-enable
```

neighbor next-hop-self (BGP)

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**

Parameters

ip-address
The IPv4 address of the neighbor.

ipv6-address
The IPv6 address of the neighbor.

peer-group-name
The peer group name configured by the **neighbor** *peer-group-name*

always
Enables this feature for route reflector (RR) routes.

Modes

BGP configuration mode.

Usage Guidelines

Use this command to cause the device to list itself as the next hop in updates that are sent to the specified neighbor.

Use the **no** form of this command to remove this configuration at BGP level.

Examples

The following example configures the device to list itself as the next hop in updates sent to a neighbor with the IP address 10.157.22.26.

```
device# config
device(config)# router bgp
device(config-bgp-router)# neighbor 10.157.22.26 next-hop-self
```

The following example configures the device to list itself as the next hop in updates sent to a neighbor that is a route-reflector client of the device.

```
device# config
device(config)# router bgp
device(config-bgp-router)# neighbor 10.157.22.26 next-hop-self always
```

net

Configures an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process.

Syntax

net *NSAP address*

no net *NSAP address*

Command Default

900 seconds (15 minutes).

Parameters

NSAP address

Specifies a Network Service Access Point (NSAP) address; composed of both an area ID and a system ID.

Modes

IS-IS router configuration mode

Usage Guidelines

The *area-id* parameter specifies the area and has the format xx or xx.xxxx. For example, 49 and 49.2211 are valid area IDs.

The *system-id* parameter specifies the device's unique IS-IS router ID and has the format xxxx.xxxx.xxxx. You can specify any value for the system ID. A common practice is to use the base MAC address of the device as the system ID. The base MAC address is also the MAC address of port 1.

You must use the same system ID in all the NETs on the device.

The **no** form of the command removes the configured NET.

Examples

The following example configures a NET that has the area ID 49.2211, the system ID 0000.00bb.cccc (the base MAC address), and the SEL value 00.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# net 49.2211.0000.00bb.cccc.00
```

next-hop-mpls

Configures BGP shortcuts using next-hop MPLS to force BGP to use an MPLS tunnel as the preferred route to a destination network when an MPLS LSP tunnel is available.

Syntax

next-hop-mpls [**compare-lsp-metric** | **follow-igp**]

no next-hop-mpls [**compare-lsp-metric** | **follow-igp**]

Command Default

BGP uses the default BGP decision process and native IP forwarding to build BGP EMCP routes. Only IP routing tables are used to resolve routes for the routing table.

Parameters

compare-lsp-metric

Enables BGP to compare the configured LSP metrics as the IGP cost for the next hop.

follow-igp

Ignores the MPLS metric cost in the BGP decision process and uses the IGP cost. BGP checks when an MPLS LSP is present, and totally ignores the LSP metric.

Modes

BGP address-family IPv4 unicast configuration mode

Usage Guidelines

When the **next-hop-mpls** command is enabled without either option, BGP sets the LSP metrics to one.

Enabling or disabling an option takes effect immediately. BGP automatically recalculates the existing BGP routes.

The **compare-lsp-metric** and **follow-igp** options are mutually exclusive.

When the **compare-lsp-metric** option is configured and you change the LSP metric, the routing table is updated.

Use the **no** form of the command to disable global next-hop MPLS.

When you use the **no** form of the command with the **compare-lsp-metric** or **follow-igp** option, all LSP metrics become equal cost. However, global next-hop MPLS remains enabled.

For the **follow-igp** option, consider the following:

- When you are running IGP throughout the network, and the IGP metric is trusted in the entire domain, you may want to rely on this IGP metric to make a best path and forwarding decision, regardless of whether the forwarding happens in native IP or MPLS encapsulation.
- The MPLS metric is manually configured in each LSP. There is no dynamic way to tie MPLS metric with an IGP metric. When using MPLS LSP as a BGP route outgoing interface, you loses the ability to tie the forwarding decision with a unified IGP metric.

When combined with the BGP **install-igp-cost** command, you can change the route cost from BGP MED to IGP cost and is used when BGP routes are added to the RTM.

When combined with a BGP outbound policy for route **set metric-type internal** command, you can set Layer-3 VPN and IP over MPLS routes using IGP metric to send out as the BGP MED value.

Examples

The following example enables BGP shortcuts through next-hop MPLS and BGP to set the next hop IGP cost to one instead of the actual LSP metric.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# next-hop-mpls
```

The following example enables BGP shortcuts through next-hop MPLS and BGP to use the configured LSP metrics as the IGP cost for the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# next-hop-mpls compare-lsp-metric
```

The following example enables BGP shortcuts through next-hop MPLS and BGP to ignore the LSP metrics and to use the IGP cost for the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# next-hop-mpls follow-igp
```

non-preempt-mode

Enables the non-preempt mode on all backups.

Syntax

non-preempt-mode

no non-preempt-mode

Command Default

By default, the non-preempt mode is disabled; preemption is enabled.

Modes

VRID configuration mode

Usage Guidelines

By default, a backup that has a higher priority than another backup that has become the master can preempt the master, and take over the role of master. If you want to prevent this behavior, disable preemption.

Preemption applies only to backups and takes effect only when the master has failed and a backup has assumed ownership of the VRID. The **non-preempt-mode** command prevents a backup with a higher priority from taking over as master from another backup that has a lower priority but has already become the master of the VRID.

Preemption is especially useful for preventing flapping in situations where there are multiple backups and a backup with a lower priority than another backup has assumed ownership, because the backup with the higher priority was unavailable when ownership changed.

If you enable the non-preempt mode (thus disabling the preemption feature) on all the backups, the backup that becomes the master following the disappearance of the master continues to be the master. The new master is not preempted.

The **no** form of the command disables the non-preempt mode.

Examples

The following example enables the non-preemption mode.

```
device(config)# vlan 200
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# non-preempt-mode
```

non-preempt-mode (VRRP)

Disables preempt mode for a Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) backup device.

Syntax

non-preempt-mode

no non-preempt-mode

Command Default

Preemption is enabled by default.

Modes

VRID interface configuration mode

Usage Guidelines

This command is supported in VRRP and VRRP-E. When the **non-preempt-mode** command is entered, a backup device with a higher VRRP priority is prevented from taking control of the virtual router ID (VRID) from another backup device that has a lower priority, but has already assumed control of the VRID. Disabling preemption is useful to prevent flapping when there are multiple backup devices and a backup with a lower priority assumes the role of master. When other backup devices with a higher priority are back online, the role of master can flap between devices.

In VRRP, the owner device always assumes the role of master when it comes back online, regardless of the preempt mode setting.

Enter **no non-preempt-mode** to re-enable preemption.

Examples

The following example disables preempt mode for the virtual-router ID 1 session:

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.3/24
device(config-if-e1000-1/5)# ip vrrp vrid 1
device(config-if-e1000-1/5-vrid-1)# non-preempt-mode
```

nonstop-routing (IS-IS)

Enables nonstop routing (NSR) for Intermediate System-to-Intermediate System (IS-IS).

Syntax

nonstop-routing

no nonstop-routing

Command Default

Enabled

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command disables nonstop routing.

Examples

The following example enables NSR for IS-IS on a device.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# nonstop-routing
```

The following example disables NSR for IS-IS on a device.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no nonstop-routing
```

nonstop-routing (OSPF)

Enables nonstop routing (NSR) for OSPF.

Syntax

nonstop-routing

no nonstop-routing

Command Default

Enabled.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command disables non-stop routing.

Examples

The following example re-enables NSR on a device.

```
device# configuration terminal
device(config)# router ospf
device(config-ospf-router)# nonstop-routing
```

notification-timer

Sets the length of the EOL notification timer for LDP-IGP synchronization.

Syntax

notification-timer *milliseconds*

no notification-timer *milliseconds*

Command Default

The default value is 60000 milliseconds.

Parameters

milliseconds

Specifies the length of the EOL notification timer in milliseconds. Enter an integer from 100 to 120000.

Modes

MPLS LDP end-of-lib (eol) configuration mode

Usage Guidelines

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

Examples

The following example configures the EOL notification timer to 80000 milliseconds.

```
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# end-of-lib
device(config-mpls-ldp-eol)# notification-timer 80000

device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# eol
device(config-router-mpls-ldp-eol)# notification-timer 80000
```

ocsp-url

Sets the Online Certificate Status Protocol (OCSP) URL name to determine the revocation state of a certificate.

Syntax

ocsp-url *URL name*

no ocsp-url *URL name*

Parameters

URL name
The OSCP URL name.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The **no** form of the command removes the OCSP URL name.

Examples

The following example specifies the OCSP URL name as provided here.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# ocsp-url http://WIN-HJ98AK136A0.englab.brocade.com/ocsp
```

History

Release version	Command history
5.9.00	This command was introduced.

openflow controller source-interface

Configures a source-interface for the connection from the device to the controller.

Syntax

openflow controller source-interface { **ethernet** *slot/port* | **loopback** *number* | **ve** *number* } **force-reconnect**

no openflow controller source-interface { **ethernet** *slot/port* | **loopback** *number* | **ve** *number* } **force-reconnect**

Command Default

The CLI command is applicable only when the device is in active mode. The device initiates connection to the remote OpenFlow controller.

Parameters

ethernet *slot port*

Gives information about a particular slot and port in an internet

loopback *number*

Specifies a loopback interface.

ve *number*

Specifies a virtual interface.

force-reconnect

Forces the existing connections to use the newly configured source-interface.

Modes

Privileged EXEC mode

Usage Guidelines

When adding a new controller to the device, a connection will be attempted to the controller IP address using the configured source-interface. If the source-interface has no IP address configured or the interface is down, the syslog messages will be generated and a connection attempt will be made again in 15 seconds.

Examples

To see the source-interface, use this command.

```
device(config)#openflow controller ?
  ip-address          Set the Controller IPv4 address
  passive             Configure passive connection mode
  source-interface    Set the Source Interface to be used for controller
                      connections

If a new controller is added after this, routing table will be used to connect to the controller.

Device(config)#openflow controller source-interface ?
  ethernet       Ethernet interface
  loopback       Loopback interface
  ve             Virtual Ethernet interface
```

For a specified ethernet interface, use this command.

```
device(config)#openflow controller source-interface ethernet 2/2?
  force-reconnect   Force the existing connections to use the newly configured
                    source-interface
```

History

Release version	Command history
5.8.00	This command was introduced.

openflow enable

Enables or disables the OpenFlow hybrid port-mode on the port.

Syntax

openflow enable [**layer2** | **layer3** | **layer23** [**hybrid-mode**]]

no openflow enable [**layer2** | **layer3** | **layer23** [**hybrid-mode**]]

openflow enable ofv130 [**acl-pbr**]

no openflow enable ofv130 [**acl-pbr**]

Parameters

layer2
Enables Layer 2 matching mode for flows.

layer3
Enables Layer 3 matching mode for flows.

layer23 hybrid-mode
Enables Layer 2 and Layer 3 matching mode for flows with an option for hybrid port-mode.

acl-pbr
Enables ACL or PBR on OpenFlow interfaces at global level.

Modes

Global configuration mode.

Interface configuration mode.

Usage Guidelines

In interface configuration mode, this command enables Layer 2 or Layer 3 matching mode for flows with an optional enabling of hybrid port-mode.

NOTE
OpenFlow must be globally enabled before the Layer 2 or Layer 3 matching modes can be specified.

Examples

After OpenFlow 1.3 is enabled, the following example configures Layer 2 and Layer 3 matching mode for flows.

```
device# configure terminal
device(config)# openflow enable ofv130
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# openflow enable layer 23
```

History

Release	Command History
6.1.00	This command was modified to display OpenFlow ACL and PBR information.
5.6.00	This command was modified to display OpenFlow hybrid port mode information.

openflow hello-reply disable

Allows the second Hello message (Hello-reply) to be disable on the OpenFlow Controller.

Syntax

openflow hello-reply disable

Command Default

This command needs to be run and saved when connecting to the OpenFlow Controller and any other controllers by default.

Modes

EXEC and Privileged EXEC mode

Global configuration mode

Usage Guidelines

When the OpenFlow Controller receives the Hello message that the controller sent, it replies with another Hello message using the same transaction-ID as in the received Hello message.

Examples

```
device(config)# openflow ?
  controller         Configure controller
  default-behavior   Default forwarding for no match packets
  enable             Enable/disable OpenFlow
  hello-reply        Configure HELLO Reply for HELLO originated from Controller

device(config)# openflow hello-reply ?
  disable   Disable HELLO Reply from the switch/router

device(config)# openflow hello-reply disable ?

device# show openflow
Administrative Status:       Enabled
SSL Status:                  Enabled
Source-Interface:            Not Configured
Source-Interface Status:     NA

Controller Type:             ofv130
HELLO Reply:                 disabled
Number of Controllers:       2
……

device# show running-config | i openflow
openflow enable ofv130
openflow hello-reply disable
```

History

Release version	Command history
NI05.7.00	This command was introduced.

org-name

Configures the organization name for the Public Key Infrastructure (PKI) entity.

Syntax

org-name *string*

Parameters

string

Specifies name of the organization for the PKI entity.

Modes

PKI entity configuration mode.

Examples

The following example configures the organization for PKI entity.

```
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# org-name Brocade
```

History

Release version	Command history
5.8.00	This command was introduced.

org-unit-name

Configures the unit name of the organization to which the Public Key Infrastructure (PKI) entity belongs to.

Syntax

org-unit-name *string*

Parameters

string

Specifies unit name of the organization for PKI entity.

Modes

PKI entity configuration mode.

Examples

The following example configures unit of the organization the PKI entity belongs to.

```
device configure terminal
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# org-unit-name routing
```

History

Release version	Command history
5.8.00	This command was introduced.

owner

Designates a virtual router as the Virtual Router Redundancy Protocol (VRRP) owner and configures priority and track values.

Syntax

owner [**priority** *value*] [**track-priority** *value*]

no owner [**priority** *value*] [**track-priority** *value*]

Command Default

No virtual routers are designated as the VRRP owner.

Parameters

priority *value*

Abdicates owner status by setting a value that is lower than the backup default priority value. Value can be from 1 to 254. Default is 100.

track-priority *value*

Sets the priority value if the tracked port fails. Value can be from 1 to 254. Default is 2.

Modes

VRID interface configuration mode

Usage Guidelines

This command specifies that the device on which it is configured owns the IP address that is associated with the virtual router; making this device the default VRRP master router with its priority set to 255.

This command must be entered before the **ip-address** command can be configured for a VRRP virtual router ID (VRID).

The **no** form of this command removes the virtual router configuration.

Examples

The following example configures the device as the VRRP owner.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
```

The following example configures the device as the VRRP owner and sets the track priority to 10.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner track-priority 10
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
```

partial-spf-interval

Changes the partial shortest path first (PSPF) interval.

Syntax

partial-spf-interval *max-wait initial-wait second-wait*

no partial-spf-interval

Parameters

max-wait

Specifies the maximum interval in seconds between SPF recalculations. The range is from 0 through 120 seconds. The default is 5 seconds.

initial-wait

Specifies the initial SPF calculation delay in milliseconds after an LSP change. The range is from 0 through 120000 milliseconds. The default for this variable is value of the *max-wait* time.

second-wait

Indicates the hold time between the first and second SPF calculation in milliseconds. The range is from 1 through 120000 milliseconds. The default is 5000 milliseconds (5 seconds). The default for this variable is value of the *max-wait* time.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example specifies that the maximum interval between SPF recalculations is 15 seconds, the initial SPF calculation delay is 10000 milliseconds, and the hold time between the first and second SPF calculation is 15000 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# partial-spf-interval 15 10000 15000
```

The following example restores the default values.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no partial-spf-interval
```

permit (arp-guard-access-list)

Specifies the required set of ACL rules and filters for an associated ARP guard group.

Syntax

permit *vlan-id src-ip-address* [*src-mac-address* | **any**]

no permit *vlan-id src-ip-address* [*src-mac-address* | **any**]

Command Default

If this command is not entered, no ACL rules or filters are associated with an ARP guard group.

Parameters

vlan-id

Specifies a VLAN ID in the range between 1 and 4090.

src-ip-address

Specifies a source IP address.

src-mac-address

Specifies a source MAC address.

any

Specifies all addresses.

Modes

ARP-Guard access-list name mode.

Usage Guidelines

The **no** form of the command removes the rules and filters for the specific ARP guard group.

Examples

The following command example specifies the required set of ACL rules and filters for the AS201 ARP guard group.

```
device# configure terminal
device(config)# arp-guard-access-list AS201
device(config-arp-guard-access-list-AS201)#permit 100 1.2.3.4 1111.2222.3333
```

History

Release version	Command history
5.7.00	This command was introduced.

permit (IPv6 ACL rules)

Inserts permit filtering rules into IPv6 ACLs. These rules permit traffic according to source and destination addresses, port protocol, and other IPv6 frame content.

Syntax

Use the following syntax to define a TCP rule:

permit [**enable-accounting**] [**vlan** *vlan-id*] **tcp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**established**] [**syn**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to define an ICMP rule:

permit [**enable-accounting**] [**vlan** *vlan-id*] **icmp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*icmp-parameters*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to define an SCTP or UDP rule:

permit [**enable-accounting**] [**vlan** *vlan-id*] { **sctp** | **udp** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to define an AHP, ESP, or IPv6 rule:

permit [**enable-accounting**] [**vlan** *vlan-id*] { **ahp** | **esp** | **ipv6** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**] [**sequence** *num*]

Use the following syntax to delete a rule, specifying the sequence number.

no permit sequence *num*

Use the following syntax to delete a TCP rule without specifying the sequence number:

no permit [**enable-accounting**] [**vlan** *vlan-id*] **tcp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**established**] [**syn**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Use the following syntax to delete an ICMP rule without specifying the sequence number:

no permit [**enable-accounting**] [**vlan** *vlan-id*] **icmp** { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*icmp-parameters*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Use the following syntax to delete an SCTP or UDP rule without specifying the sequence number:

no permit [**enable-accounting**] [**vlan** *vlan-id*] { **sctp** | **udp** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } [*source-operators*] {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [*destination-operators*] [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Use the following syntax to delete an AHP, ESP, or UDP rule without specifying the sequence number:

no permit [**enable-accounting**] [**vlan** *vlan-id*] { **ahp** | **esp** | **ipv6** } { *ipv6-source-prefix* **/** *prefix-length* | **any** | **host** *source-ipv6_address* } {*ipv6-destination-prefix* **/** *prefix-length* | **any** | **host** *ipv6-destination-address* } [**drop-precedence** *dp-value*] [**drop-precedence-force** *dp-value*] [**dscp** *dscp-value*] [**dscp-marking** *dscp-value*] [**priority-force** *number*] [**priority-mapping** *802.1p-value*] [**fragments**] [**routing**] [**match-payload-length**] [**suppress-rpf-drop**] [**log**] [**log-input**] [**mirror**] [**copy-sflow**]

Parameters

enable-accounting

(Not supported on Brocade MLX Series or Brocade NetIron XMR Series devices.) Enable accounting for the rule.

vlan *vlan-id*

(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.) Specify a VLAN.

protocol

Specifies the type of IPv6 packet you are filtering. You can either specify a protocol number (from 0 through 255) or one of the following protocol names:

- AHP—Authentication Header
- ESP—Encapsulating Security Payload
- ICMP—Internet Control Message Protocol
- IPv6—Internet Protocol, version 6
- SCTP—Stream Control Transmission Protocol
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol

ipv6-source-prefix **/** *prefix-length*

Specifies a source prefix and prefix length that a packet must match for the specified action (deny or permit) to occur. You must specify the *ipv6-source-prefix* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. Specify the *prefix-length* parameter as a decimal value, preceded by a slash mark (/).

any

When specified instead of the *ipv6-source-prefix*/*prefix-length* or *ipv6-destination-prefix*/*prefix-length* parameters, matches any IPv6 prefix and is equivalent to the IPv6 prefix::/0.

host *source-ipv6_address num*

Enables you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

source-operators and *destination-operators*

If you specified **sctp**, **tcp**, or **udp** protocol, the following optional operators are available:

eq

The policy applies to the port name or number you enter after **eq**.

gt

The policy applies to 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 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 port numbers except the port number or port name you enter after **neq**.

range

The policy applies to all port numbers that are between the first 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.

ipv6-destination-prefix **/** *prefix-length*

Specifies a destination prefix and prefix length that a packet must match for the specified action (deny or permit) to occur. You must specify the *ipv6-destination-prefix* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. Specify the *prefix-length* parameter as a decimal value, preceded by a slash mark (/).

icmp-parameters

If you specify **icmp** as protocol, many parameters are available. For a current list, type a question mark (?) at the command prompt.

icmp-message-type

Specifies an ICMP message type. Values range from 0 through 255.

drop-precedence *dp-value*

Filters by the drop-precedence value that you specify. Values range from 0 through 3.

drop-precedence-force *dp-value*

If there are conflicting priority values for ingress packets, the default action is a priority merge. However, **drop-precedence-force** assigns the specified value to matching traffic. Values range from 0 through 3.

dscp *dscp-value*

The policy applies to packets that match DSCP value. Values range from 0 through 63.

dscp-marking *dscp-value*

Assigns the value that you specify to the packet. Values range from 0 through 63.

priority-force *number*

Forces outgoing priority. Values range from 0 through 7.

priority-mapping *802.1p-value*

Filters by 802.1p priority.

established

(For TCP rules only) Filter packets that have the ACK (Acknowledgment) or RST (Reset) flag set. This policy applies only to established TCP sessions, not to new sessions.

syn

(For TCP rules only) Filter packets with the SYN (Synchronize) flag set.

fragments
(Not applicable for filtering based on source port, destination port, TCP protocol, or ICMP protocol) The policy applies to fragmented packets that contain a non-zero fragment offset.

routing
(Not applicable for filtering based on source port, destination port, TCP protocol, or ICMP protocol) The policy applies only to IPv6 source-routed packets.

match-payload-length
(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.) Match packets for configured IP payload length.

suppress-rpf-drop
(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices.) Permit packets that fail the IPv6 RPF check.

log
Logs entries that match rule criteria.

log
(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices) Enables inbound logging for the rule. An additional requirement for logging is that the **ipv6 traffic-filter enable-permit-logging** command be in effect.

log-input
(Not supported on Brocade NetIron CER Series or Brocade NetIron CES Series devices) Enables inbound logging for the rule, with log entries including the incoming interface. An additional requirement for logging is that the **ipv6 traffic-filter enable-permit-logging** command be in effect.

copy-sflow
Sends matching inbound packets to the sFlow collector.

sequence *num*
Enables you to assign a sequence number to the rule. If you do not specify **sequence** *num*, the rule is added at the end of the list.

Modes

ACL configuration mode

Usage Guidelines

If you need to specify **sequence** *num*, you can do so in one of the following syntax positions:

- As the first element
- At any point following the destination specification.

Examples

The following example defines rules that filter by the SCMP protocol.

```
device# configure terminal
device(config# ipv6 access-list sctp_filter
device(config-ipv6-access-list sctp_filter)# permit sctp 201:1::1:1/64 eq 28 any range 10 100
device(config-ipv6-access-list sctp_filter)# permit sctp 201:1::1:1/64 lt 28 301:1::1:1/64 gt 100
device(config-ipv6-access-list sctp_filter)# deny sctp any lt 28 any gt 100
```

The following example shows how the keyword to specify a mask is added to all the places in the ACL configuration template where the IPv6 address prefix is present.

```
device configure terminal
device(config)# ipv6 access-list temp
device(config-ipv6-access-list temp)# permit ipv6
device(config-ipv6-access-list temp)# permit ipv6 1::1
device(config-ipv6-access-list temp)# permit ipv6 1::1 f::f
device(config-ipv6-access-list temp)# permit ipv6 1::1 f::f 2::2
```

The following example shows the IPv6 wildcard match configuration.

```
device# configure terminal
device(config)# ipv6 access-list wildcard
device(config-ipv6-access-list wildcard)# permit ipv6 ?
     X:X::X:X/M       IPv6 source prefix
     X:X::X:X         IPv6 source address
     any              Any source host
device(config-ipv6-access-list wildcard)# permit ipv6 1000::1 ?
     X:X::X:X         IPv6 source wildcard mask
device(config-ipv6-access-list wildcard)# permit ipv6 1000::1 ::FFFF:0 ?
     X:X::X:X/M       IPv6 destination prefix
     X:X::X:X         IPv6 destination address
     any              Any destination host
     host             A single destination host
device(config-ipv6-access-list wildcard)# permit ipv6 1000::1 ::FFFF:0 2000::1 ?
     X:X::X:X         IPv6 destination wildcard mask
device(config-ipv6-access-list wildcard)#permit ipv6 1000::1 ::FFFF:0 2000::1 ::FFFF:0:0
```

History

Release version	Command history
6.0.00a	This command was modified to support the SCTP protocol.

pim neighbor-filter

filters the neighbor routers on an interface.

Syntax

[ip | ipv6] pim neighbor-filter *aclname*

no [ip | ipv6] pim neighbor-filter *aclname*

Parameters

acl name Filters neighbor to participate in PIM.

Modes

Global configuration mode.

EXEC mode.

Privileged EXEC mode.

Command Output

The **pim neighbor-filter** command is used on an interface to filter the neighbor routers.

Examples

```
device configure terminal
device(config)# interface ethernet 1/3
device(config-if-e1000-1/3)#  ip pim neighbor-filter 10
device(config-if-e1000-1/3)#  ipv6 pim neighbor-filter f10
```

History

Release	Command History
5.5.00	This command was added to filter the neighbor router on the interface.

ping mpls ldp

Sends an MPLS echo request from the ingress to the egress LSR.

Syntax

ping mpls ldp { *ip_addr* | **ip_addr/mask-_length** } [**count** *num* | **destination** *ip_addr* | **detail** | **nexthop** *ip_addr* | **reply-mode** [*no_reply* | *router_alert*] | **reply-tos** *num* | **size** *bytes* | **source** *ip_addr* | **timeout** *msec*]

Parameters

ip_addr

Specifies the LDP IPv4 FEC destination prefix.

ip_addr/mask_length

Specifies the LDP IPv4 destination prefix and mask length. If the mask-length is not specified, the default value is 32.

count *num*

Specifies the number of echo requests to send. Values are from 1 to 4294967294. The default value is five.

destination *ip_addr*

Specifies an IP address within the 127/8 subnet. The default address is 127.0.0.1.

detail

Displays the details of the echo request and reply messages. By default, the display is in the brief mode.

nexthop *ip_addr*

The next closest router a packet can go through. The nexthop IPv4 address to send the OAM request to. If an address that does not match the outgoing path for the tunnel is given, following error message appears as the response:**Ping fails: LDP next-hop does not exist.**

reply-mode

Specifies the reply mode field in the echo request only if the user does not want the reply to be sent as an IPv4 UDP packet.

no_reply

Use to test one-way connectivity.

router_alert

Use when the normal IP return path is unreliable. This option indicates that the reply must be sent as an IPv4 UDP packet with the Router Alert option. This option requires extra overhead processing at each LSR along the return path.

reply-tos *num*

Specifies a TOS value between 0 and 254 to include in the Reply-TOS-byte TLV. By default, the reply-tos TLV is not included in the echo request. The last bit of the TOS byte is always 0.

size *bytes*

Specifies that the size of the echo request, including the label stack, to send. The pad TLV is used to fill the echo request message to the specified size. The minimum packet size is 80 bytes for an LDP echo request. The maximum packet size is the size of the LSP MTU.

source *ip_addr*

Specifies the IP address of any interface. Use this address as the destination address for the echo reply address. The default address is the LSR ID.

timeout *msec*

Specifies an interval in milliseconds for the echo request message. The value range is from 50 to 300000. The default timeout is 5 seconds. The maximum timeout value is 5 minutes.

Modes

Global configuration mode.

Usage Guidelines

NOTE

Once an outgoing path is chosen to send the ping request, it is not changed. Disabling the path does not cause the ping packet to be sent over other ECMP paths. Upon disabling the path, the ping operation stops because the path is down. This is the expected behavior.

Examples

The following example displays how to perform the LSP LSP ping operation.

```
device# ping mpls ldp 10.22.22.22
Send 5 80-byte MPLS Echo Requests for LDP FEC 10.22.22.22/32, timeout 5000 msec
Type Control-c to abort
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max=0/1/1 ms.
device#
```

History

Release	Command history
5.6.00	**nexthop** *ipv4-address* is added to the existing **ping** command.

pki authenticate

Authenticates a certification authority (CA) to a device by using the self-signed certificate of the CA.

Syntax

pki authenticate *trustpoint-name*

Parameters

trustpoint-name

Specifies the CA or trustpoint name.

Modes

Global configuration mode

Usage Guidelines

The behavior of this command is affected by the enrollment terminal status of the trustpoint. Enrollment terminal is enabled and disabled by using the **enrollment terminal** command.

- By default, enrollment terminal is disabled and a CA certificate is requested and returned from the CA server over HTTP.
- When enrollment terminal is enabled, a CA certificate (which has been downloaded from an offline CA server) is imported by way of pasting onto the device terminal and confirming the fingerprint. In the case of chain validation, multiple CA certificates are pasted onto the device terminal, one after another.

This command authenticates the CA by using the self-signed certificate of the CA that contains the public key of the CA. Since the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator before you run this command. Authentication is done by manually verifying the fingerprint of the self-signed certificate on the terminal. This command is saved to the router configuration and the certificates are saved to the router.

Examples

The following example authenticates a CA named brocade.

```
device configure terminal
device(config)# pki authenticate brocade
```

The following example authenticates a CA named example_tp by pasting the CA certificate on the device terminal.

```
device(config)# pki trustpoint example_tp
device(config-pki-trustpoint-mytp)# enrollment terminal
device(config-pki-trustpoint-mytp)# exit
device(config)# pki authenticate example_tp

Enter certificate in base64 encoded format.
End with a blank line.

-----BEGIN CERTIFICATE-----
MIIDEzCCArqgAwIBAgIJAMYEw0fMnyOpMAoGCCqGSM49BAMCMIGMMQswCQYDVQQG
EwJVUzELMAkGA1UECBMCTUQxFDASBgNVBAcTC0NhdG9uc3ZpbGxlMQwwCgYDVQQK
EwNHU1MxKzApBgkqhkiG9w0BCQEWHHJvb3RjYS1lY2RzYUBnb3NzYW1lcnNlYy5j
b20xHzAdBgNVBAMTFkdvc3NhbWVyIEVDRFNBIFJvb3QgQ0EwHhcNMTUwNjE5MTY0
NjI4WhcNMjUwNjE2MTY0NjI4WjCBjDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1E
MRQwEgYDVQQHEwtDYXRvbnN2aWxsZTEMMAoGA1UEChMDR1NTMSswKQYJKoZIhvcN
AQkBFhxyb290Y2EtZWNkc2FAZ29zc2FtZXJzZWMuY29tMR8wHQYDVQQDExZHb3Nz
YW1lciBFQ0RTQSBSb290IENBMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEIKpj
7bRTde6IjMB/5I0YfQA5tbugpeMFOSQv7FwiGS9wH+Ie49s5N6AcRZnqDxjabEaD
qdroVG+tv0PEuaWd7KOCAQEwgf4wHQYDVR0OBBYEFOyftp0utn4K/0BY0xxT5yWP
1MxYMIHBBgNVHSMEgbkwgbaAFOyftp0utn4K/0BY0xxT5yWP1MxYoYGSpIGPMIGM
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxFDASBgNVBAcTC0NhdG9uc3ZpbGxl
MQwwCgYDVQQKEwNHU1MxKzApBgkqhkiG9w0BCQEWHHJvb3RjYS1lY2RzYUBnb3Nz
YW1lcnNlYy5jb20xHzAdBgNVBAMTFkdvc3NhbWVyIEVDRFNBIFJvb3QgQ0GCCQDG
BMNHzJ8jqTAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjAKBggqhkjOPQQDAgNH
ADBEAiAUXYCIZRZaHztfQ/YHKSaDH49IsOqNxFTkm9ojz7QAEgIgGMua7Ww53dXJ
Tc8S1Bkbkh5GN/zuybCMHQ1ioqSME1w=
-----END CERTIFICATE-----

The self signed certificate has fingerprint:c5:15:e8:27:7e:5d:1b:e0:66:df:ca:3e:18:40:ff:9e:f1:9d:a3:ec
Do you accept this certificate as root CA certificate? (enter 'y' or 'n'): y
you accepted the certificate.

Do you wish to enter more ca certificates? (enter 'y' or 'n'): y
Enter certificate in base64 encoded format.
End with a blank line.

-----BEGIN CERTIFICATE-----
MIIDfTCCAySgAwIBAgIBAjAKBggqhkjOPQQDAjCBjDELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk1EMRQwEgYDVQQHEwtDYXRvbnN2aWxsZTEMMAoGA1UEChMDR1NTMSsw
KQYJKoZIhvcNAQkBFhxyb290Y2EtZWNkc2FAZ29zc2FtZXJzZWMuY29tMR8wHQYD
VQQDExZHb3NzYW1lciBFQ0RTQSBSb290IENBMB4XDTE1MDYxOTE2NDYyOVoXDTI1
MDYxNjE2NDYyOVowgZYxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNRDEUMBIGA1UE
BxMLQ2F0b25zdmlsbGUxDDAKBgNVBAoTA0dTUzEkMCIGA1UEAxMbR29zc2FtZXIg
RUNEU0EtRUNEU0EgU3ViIENBMTAwLgYJKoZIhvcNAQkBFiFzdWJjYS1lY2RzYS1l
Y2RzYUBnb3NzYW1lcnNlYy5jb20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQR
Bq93D2C7q+w/vBRgn90h363E7SRhheFDpB6YIDDSp9S5dH501WTelqsAUzagrip1
sl8HDeqMmVuZUzSNZV0vo4IBaTCCAWUwHQYDVR0OBBYEFD1qxubtQ0QYnlmY/MLS
4a2qNuUfMIHBBgNVHSMEgbkwgbaAFOyftp0utn4K/0BY0xxT5yWP1MxYoYGSpIGP
MIGMMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUQxFDASBgNVBAcTC0NhdG9uc3Zp
bGxlMQwwCgYDVQQKEwNHU1MxKzApBgkqhkiG9w0BCQEWHHJvb3RjYS1lY2RzYUBn
b3NzYW1lcnNlYy5jb20xHzAdBgNVBAMTFkdvc3NhbWVyIEVDRFNBIFJvb3QgQ0GC
CQDGBMNHzJ8jqTAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjAyBgNVHR8EKzAp
MCegJaAjhiFodHRwOi8vMTAuMC4wLjM0L3Jvb3RjYS1lY2RzYS5jcmwwMQYIKwYB
BQUHAQEEJTAjMCEGCCsGAQUFBzABhhVodHRwOi8vMTAuMC4wLjM0Ojc3NzgwCgYI
KoZIzj0EAwIDRwAwRAIgemQ2bHWJT+8EH/ol9qDY8QGmKSb/EbKSGUnVVVrkqBIC
IEZLG8jwpnAVaT7S+Sdc2nGf600CCdcVKQp2q8QOjpmE
-----END CERTIFICATE-----

Do you wish to enter more ca certificates? (enter 'y' or 'n'): n
PKI: Trustpoint example_tp, authentication: Success

device(config)#
```

History

Release version	Command history
5.8.00	This command was introduced.
6.0.00a	This command was modified to add support for authenticating an offline CA.

pki cert validate

Validates or checks if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid.

Syntax

pki cert validate *trustpoint-name*

Parameters

trustpoint-name
Specifies the trustpoint name.

Modes

Global configuration mode.

Usage Guidelines

Use this command after loading the router certificate using the **import** command to validate the router certificate.

The following files must be downloaded first to the MP flash drive using TFTP and then imported into the system software using the **import** command:

- CA/trustpoint certificate
- Router certificate
- Router private key

Examples

The following example configures validation of a trustpoint.

```
device(config)# pki cert validate brocade
```

History

Release version	Command history
5.8.00	This command was introduced.

pki enroll

Generates a certificate signing request (CSR) that is used to enroll the device on the certification authority (CA) trustpoint. A CSR can be generated for an online or offline trustpoint.

Syntax

pki enroll *name*

no pki enroll *name*

Command Default

By default, this command is not configured.

Parameters

name

Specifies the CA trustpoint for which the CSR is to be generated.

Modes

Global configuration mode

Usage Guidelines

The behavior of this command is affected by the enrollment terminal status of the trustpoint. Enrollment terminal is enabled and disabled by using the **enrollment terminal** command.

- By default enrollment terminal is disabled and the Simple Certificate Enrollment Protocol (SCEP) protocol is used to generate the CSR in PKCS #7 format and send it to the CA server over HTTP. The CA server then processes the CSR and returns the SCEP response which contains the client certificates. The requested certificates are added for each key pair on the Brocade MLXe Series device. The requested certificates are saved to the device, but the **pki enroll** *name* command is not saved as part of the device configuration. When enrollment terminal is disabled, the **no** form of the command removes the certificates from the device.
- When enrollment terminal is enabled, the CSR is displayed (in PKCS #10 format) on the device terminal and saved as a PEM-encoded file in flash memory so that it can be copied and transported to the CA server to obtain the client certificates. The client certificates are transported back and manually imported into the Brocade MLXe Series device. When enrollment terminal is enabled, the **no** form of the command has no impact.

Examples

The following example generates a CSR that is sent to a CA server named mytrustpoint.

```
device(config)# pki enroll mytrustpoint
```

The following example enables enrollment terminal for a trustpoint named example_tp and generates a CSR which is displayed on the device terminal.

```
device(config)# pki trustpoint example_tp
device(config-pki-trustpoint-example_tp)# enrollment terminal
device(config-pki-trustpoint-example_tp)# exit
device(config)# pki enroll example_tp

PKI: Certificate Request for trustpoint example_tp saved in file pki_certreq_example_tp and displayed
below:

-----BEGIN CERTIFICATE REQUEST-----
MIIBkzCCARsCAQAwWjELMAkGA1UEBhMCSU4xDDAKBgNVBAgTA0tBUjEMMAoGA1UE
BxMDQkxSMQ0wCwYDVQQKEwRCUkNEMQswCQYDVQQLEwJOSTETMBEGA1UEAxMKY2hh
aXRhbnlhMTB2MBAGByqGSM49AgEGBSuBBAAiA2IABLOY6MslGw/juGnz5hG0H7tu
fhSwM/k1QoX13Vg7RRguD2HdnRvjfzUcY/g4Fsq8nE9xAvuDwvxgA3TbCrZJys36
Rv0jNJWJ7TUfelUq4hbmzW9vCCsmbPZeH6caRWFMDqBCMB8GCSqGSIb3DQEJBzES
ExA5MjE4QjdGQ0ZFNUU4REJBMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQD
AgXgMAkGByqGSM49BAEDZwAwZAIwOSUGx0Z+IOixgVJ8QMARr4r5cpTr+xTLXaNR
zNxEfGHq/tZzKm/zYBsNhBaCwJ7JAjA+lz5Ub12bqJX688yBaYToo9lTeho0BilC
7bCvKKVWckgOWQKys85AJtf4PS1nA8U=
-----END CERTIFICATE REQUEST-----

device(config)#
```

History

Release version	Command history
5.9.00	This command was introduced.
6.0.00a	This command was modified to add support of offline certificate enrollment.

pki entity

Configures the Public Key Infrastructure (PKI) end-user parameters and enters the PKI entity configuration mode.

Syntax

pki entity *name*

Parameters

name

Specifies entity name for the PKI entity.

Modes

Global configuration mode.

Examples

The following example configures the PKI entity and enters the PKI entity configuration mode.

```
device configure terminal
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)#
```

History

Release version	Command history
5.8.00	This command was introduced.

pki export

Manually exports certificates from the specified CA trustpoint to the flash memory of the router. Export certificates after the router is rebooted to ensure the router has current, valid certificates.

Syntax

pki export *name* **pem url** *filename*

Command Default

By default, this command is not configured.

Parameters

name

Specifies the name of the CA trustpoint that has the certificates you want to export to the flash memory of the router.

pem url *filename*

Specifies the name of the file being exported to the flash memory of the router. The file contains the certificates.

Modes

Privileged EXEC mode

Usage Guidelines

NOTE

The trustpoint name you specify must match the name of the trustpoint you specified using the **pki trustpoint** command.

Use the **pki export key** command to manually export key-pairs to the router, or the **pki export crl** to manually export certificate revocation lists to the router.

Examples

This example manually exports certificates from the CA trustpoint named *mytrustpoint* to the flash memory of the router. The exported file that contains the certificates is named *file1certs*.

```
device# pki export mytrustpoint pem url file1certs
```

History

Release version	Command history
5.9.00	This command was introduced.

pki export crl

Manually exports certificate revocation lists (CRL) from the specified CA trustpoint to the flash memory of the router. Export the CRL after the router is rebooted to ensure the router has current, valid lists.

Syntax

pki export crl *trustpointname* **url** *filename*

Command Default

By default, this command is not configured.

Parameters

trustpointname

Specifies the name of the CA trustpoint that has the CRL you want to export to the flash memory of the router.

url *filename*

Specifies the name of the file being exported to the flash memory of the router. The file contains the CRL.

Modes

Privileged EXEC mode

Usage Guidelines

NOTE

The trustpoint name you specify must match the name of the trustpoint you specified using the **pki trustpoint** command.

Use the **pki export** command to manually export certificates to the router, or the **pki export key** command to manually export key-pairs to the router.

Examples

This example manually exports CRL from the CA trustpoint named *mytrustpoint* to the flash memory of the router. The exported file that contains the CRL is named *file1crl*.

```
device# pki export crl mytrustpoint url file1crl
```

History

Release version	Command history
5.9.00	This command was introduced.

pki export key

Manually exports key-pairs from the specified CA trustpoint to the flash memory of the router. Export key-pairs after the router is rebooted to ensure the router has current, valid key-pairs.

Syntax

pki export key *label password filename*

Command Default

By default, this command is not configured.

Parameters

label

Specifies the label (name) of the key-pair being exported to the flash memory of the router.

password

Specifies the password required to export key-pairs.

filename

Specifies the name of the file being exported to the flash memory of the router. The file contains the key-pair.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **pki export** command to manually export certificates to the router, or the **pki export crl** command to manually export CRL to the router.

Examples

This example manually exports the key-pair labeled *1212* from the CA trustpoint named *mytrustpoint* to the flash memory of the router. The exported file that contains the key-pair is named *file1key*, and the password is *password*.

```
device# pki export 1212 password file1key
```

History

Release version	Command history
5.9.00	This command was introduced.

pki import

Manually imports Public Key Infrastructure (PKI) client certificates or certificate revocation lists (CRLs) into a trustpoint on a device. Certificates can be imported by specifying the certificate URL. Certificates and CRLs can also be imported by way of flash memory or pasting onto the device terminal.

Syntax

pki import *trustpoint-name* { **certificate** *url* | **pem** { **terminal** | **url flash:** *file-name* } }

pki import *trustpoint-name* **crl der url flash:** *file-name*

pki import *trustpoint-name* **crl pem** { **terminal** *label* | **url flash:** *file-name* }

Command Default

By default, this command is not configured.

Parameters

trustpoint-name
Specifies the name of the certification authority (CA) to associate with the imported certificate or file. A CA is also known as a trustpoint.

certificate *url*
Specifies the URL of the client certificate to import.

pem terminal
Specifies the import of a client certificate in privacy-enhanced mail (PEM) format by pasting onto the device terminal.

pem url flash: *file-name*
Specifies the name of the client certificate file to import. The file is encoded in PEM format in flash memory.

crl
Specifies the import of a CRL file.

der url flash: *file-name*
Specifies the name of the CRL file to import. The file is encoded in distinguished encoding rules (DER) format in flash memory.

pem terminal *label*
Specifies a numeric label for the CRL file to import by pasting on to the device terminal in PEM format. The range is from 1 through 15.

pem url flash: *file-name*
Specifies the name of the CRL file to import. The file is encoded in PEM format in flash memory.

Modes

Privileged EXEC mode

Usage Guidelines

This command is saved to the running configuration.

To import a certificate by using the option to paste onto the device terminal, you must first enable enrollment terminal by issuing the **enrollment terminal** command.

After certificates or files associated with a trustpoint are manually imported, they are typically exported by using the **pki export** command. This ensures that the certificates or files can be used again when the device is rebooted.

Examples

The following example shows how to manually import a PEM-encoded client certificate named mlx2.crt that is in flash memory into a trustpoint named example_tp.

```
device# pki import example_tp pem url flash: mlx2.crt
```

The following example shows how to import a client certificate named cert by pasting on the device terminal. In this example an incorrect or incomplete certificate is pasted onto the terminal and an error message is displayed.

```
device# pki import mytp pem terminal cert

Enter certificate in base64 encoded format.
End with a blank line.

-----BEGIN CERTIFICATE-----
MIIDgDCCAyigAwIBAgITGAAAACtOFPtBtvv8ywAAAAAAKzAJBgcqhkjOPQQBMCcx
JTAjBgNVBAMTHGVuZ2xhYi1XSU4tTjZDM1IwTFVEQUotQ0EtNDUwHhcNMTUxMTE0
MDgyODU4WhcNMTYxMDAxMTQ1MzIzWjBZMQswCQYDVQQGEwJJTjEMMAoGA1UECBMD
S0FSMQwwCgYDVQQHEwNCTFIxDTALBgNVBAoTBEJSQ0QxCzAJBgNVBAsTAk5JMRIw
EAYDVQQDEwljaGFpdGFueWEwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQgDXauakg4
CIimoWBMW0xoak+aopUtOFNrywqlaTuDfGP8Mc7As2C85kBIYawjAbKcZ8dDj0zc
Widy6fGB/jQqzMCcv9FjthK7/JOSjxbNhHX4hW/mMMlMtEcFla/HGK6jggHjMIIB
3zAOBgNVHQ8BAf8EBAMCBeAwHQYDVR0OBBYEFCJnYr45VOWbfJs9wIpeY5kaVuHX
MB8GA1UdIwQYMBaAFPOwj03oTL9+tBSm3lxcvPuDAa3TMGYGA1UdHwRfMF0wW6BZ
oFeGVWh0dHA6Ly9XSU4tTjZDM1IwTFVEQUouZW5nbGFiLmJyb2NhZGUuY29tL0Nl
-----END CERTIFICATE-----

importing certificate failed.

device#
```

The following example shows how to manually import a PEM-encoded CRL file from the device terminal and specify a label "1" for the imported file.

```
device# pki import example_tp crl pem terminal 1

Enter CRL in base64 encoded format.
End with a blank line.

-----BEGIN X509 CRL-----
MIICGTCCAcECAQEwCQYHKoZIzj0EATAnMSUwIwYDVQQDExxlbmdsYWItV0lOLUhK
OThBSzEzNkEwLUNBLTEwFw0xNTExMTYxMjMwNDhaFw0xNjExMTcwMDUwNDhaMCYw
JAITGgAAAAe02n9njdqiRgAAAAAABxcNMTUxMTE2MTI0MDAwWqCCAUAwggE8MB8G
A1UdIwQYMBaAFJ3/I+5GucF3N48ryw116Pt2l5wdMBAGCSsGAQQBgjcVAQQDAgEA
MAoGA1UdFAQDAgEDMBwGCSsGAQQBgjcVBAQPFw0xNjExMTYxMjQwNDhaMIHcBgkr
BgEEAYI3FQ4Egc4wgcswgciggcWggcKGgb9sZGFwOi8vL0NOPWVuZ2xhYi1XSU4t
SEo5OEFLMTM2QTAtQ0EtMTAsQ049V0lOLUhKOThBSzEzNkEwLENOPUNEUCxDTj1Q
dWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxEQz1VbmF2YWlsYWJs
ZUNvbmZpZ0ROP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RD
bGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDAJBgcqhkjOPQQBA0cAMEQCIHK4cITc
lHRR6oqhnDxNc2nspJhkdfFK3qTP3ahIk6yaAiAPxVuIyfXIEaxjRvIqiix4T3VL
07GN+2Xe/cerwkuN7Q==
-----END X509 CRL-----

CRL imported successfully.
device#
```

History

Release version	Command history
5.8.00	This command was introduced.
6.0.00a	This command was updated to add support for manual loading of: • Certificates from the device terminal. • CRLs from the device terminal and from PEM or DER formatted files in flash memory.

pki import key ec

Enables importing the Elliptic Curve (EC) key pair from the flash file with the specified key label.

Syntax

pki import key ec *key-label* **pem url flash:** *file-name*

no pki import key ec *key-label* **pem url flash:** *file-name*

Parameters

key-label
Specifies the key label name.

pem
Specifies .pem file name used to import.

url flash: *file-name*
Specifies the flash file name.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command cancels the import request that was enabled earlier.

Examples

The following example enables importing the EC key pair from the flash file with the specified key label.

```
deviceconfigure terminal
device(config)# pki import key ec brocade pem url flash: mlx2_eckey.pem
```

History

Release version	Command history
5.8.00	This command was introduced.

pki profile-enrollment

Creates a PKI enrollment profile you can use to efficiently enroll requester systems. Systems you enroll using the profile have the same You name the profile and specify the profile settings using command parameters.

Syntax

pki profile-enrollment *name* **authentication-url** *url-string* **authentication-command** *url-string* **enrollment-url** *url-stringpassword*

no pki profile-enrollment *name* **authentication-url** *url-string* **authentication-command** *url-string* **enrollment-url** *url-stringpassword*

Command Default

By default, this command in not configured.

Parameters

name

Specifies the name of the enrollment profile.

authentication-url *url-string*

Specifies the URL of the certification authority (CA) server you want to receive the authentication requests. Make sure you use the correct form of the URL.

authentication-command *string*

Specifies the HTTP command that is sent to the certification authority (CA) for authentication.

enrollment-url *url-string*

Specifies the URL of the certification authority (CA) server you want to receive the enrollment requests. Make sure you use the correct form of the URL.

password

Specifies the password for the SCEP challenge used to revoke the requester's current certificate and issue another certificate for auto mode. Copy the password from the server.

Modes

Global configuration mode (to enter the command)

Pki-profile mode (to specify parameter values)

Usage Guidelines

Use the **no** form of this command to delete all information defined in the enrollment profile.

Entering the **pki profile-enrollment** command automatically enters pki-profile mode, which is required to specify the command parameter values.

NOTE
You must specify the authentication and enrollment URLs in the correct form. The URL argument must be in the form `http://CA_name`, where CA_name is the host Domain Name System (DNS) name or the IP address of the CA.

Examples

This example creates an enrollment profile named profileA. The values for the parameters are:

- **authentication-url**: http://win-ab12aaa123a1.lab.myco.com/CertServer/mscep/mcse
- **authentication-command**: win-as12aa123a1.lab.myco.com_lab-WIN-A1B1A1BBBB
- **enrollment-url**: http://win-ab12aaa123a1.lab.myco.com/CertServer/mscep/mscep
- **password**: 1B1111AB111A2222

```
 device(config)# pki profile-enrollment profileA
                                  device(config-pki-profile)# authentication-url http://win-
ab12aaa123a1.lab.myco.com/CertServer/mscep/mcse
         device(config-pki-profile)# authentication-command win-as12aa123a1.lab.myco.com_lab-WIN-
A1B1A1BBBB
         device(config-pki-profile)# enrollment-url http://win-ab12aaa123a1.lab.myco.com/CertServer/
mscep/mscep
         device(config-pki-profile)# 1B1111AB111A2222
```

History

Release version	Command history
5.9.00	This command was introduced.

pki trustpoint

Configures the trustpoint used in all the relevant parameters needed for communication and enters the Public Key Infrastructure (PKI) trustpoint configuration mode.

Syntax

pki trustpoint *name*

no pki trustpoint *name*

Parameters

name

Specifies the PKI trustpoint name.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command deletes all the certificates associated with this Certificate Authority (CA). The trustpoint can be a self-signed root CA or a subordinate CA.

Examples

The following example configures the PKI trustpoint and enters the PKI trustpoint configuration mode.

```
device configure terminal
device(config)# pki trustpoint brocade
device(config-pki-trustpoint-brocade)#
```

History

Release version	Command history
5.8.00	This command was introduced.

pki-entity

Configures the Public Key Infrastructure (PKI) entity parameter to be used while enrolling to a CA.

Syntax

pki-entity *entity-name*

Parameters

entity-name

Specifies the entity name for the PKI entity.

Modes

PKI trustpoint configuration mode.

Examples

The following example configures the PKI entity and enters the PKI trustpoint configuration mode.

```
device configure terminal
device(config)# pki trustpoint brocade
device(config-pki-trustpoint-brocade)# pki-entity brocade-entity
```

History

Release version	Command history
5.8.00	This command was introduced.

port

Adds member ports to the transparent VLAN flooding (TVF) domain.

Syntax

port ethernet *slot/port* [**to** *slot/port* | [**ethernet** *slot/port* **to** *slot/port* | **ethernet** *slot/port*] ...]

no port ethernet *slot/port* [**to** *slot/port* | [**ethernet** *slot/port* **to** *slot/port* | **ethernet** *slot/port*] ...]

Command Default

The TVF domain does not have member ports.

Parameters

ethernet *slot/port*

Specifies an Ethernet interface to be added to the TVF domain.

to *slot/port*

Specifies a range of Ethernet interfaces to be added to the TVF domain.

Modes

TVF domain configuration mode

Usage Guidelines

The number of ports in the LAG that can be added to the TVF domain is limited based on the maximum FID pool size configured using the **system-max tvf-lag-lb-fid-group** command.

The **no** form of the command removes the member ports added to the TVF domain.

Examples

The following example adds member ports to the TVF domain.

```
device# configure terminal
device(config)# tvf-domain 1
device(config-tvf-domain-1)# port ethernet 1/1 ethernet 2/1
```

History

Release version	Command history
6.0.00	This command was introduced.

port-primary-dynamic

Enables the user to dynamically select the primary port for a link aggregation group (LAG) at the LAG configuration level.

Syntax

port-primary-dynamic

no port-primary-dynamic

Command Default

The primary port at the LAG level is enabled by default. The command is effective only when the global **lag port-primary-dynamic** command is configured.

Modes

LAG configuration mode

Usage Guidelines

The **no** form of the command disables the feature to dynamically select a primary port for the specific LAG. The **no** form of the command takes precedence over the global **lag port-primary-dynamic** command.

NOTE

The port that is to be added to the LAG should have the same speed and configuration as the existing LAG members. Dynamic primary port selection is available on Brocade NetIron MLX series devices only. To find the full description of dynamic port selection, including the prerequisites and limitations, refer to the specific chapter and topics in the *NetIron Switching Configuration Guide*.

Examples

The following example enables dynamic selection of the primary port in a LAG named "blue" at the LAG configuration level.

```
device(config)# lag blue
device(config-lag-blue)# port-primary-dynamic
```

The following example verifies that the primary port has changed from 1/1 to 3/3.

```
device(config-lag-test)# show running-configuration lag test
!
lag port-primary-dynamic
lag "test" dynamic id 10
 ports ethernet 1/1 to 1/4 ethernet 3/1 to 3/4
 primary-port 1/1
 deploy
!
!

Change primary port
====================

device(config-lag-test)# primary-port 3/3

SYSLOG: <14>Jul 18 12:47:57 LAG: test (id=10) , Configured primary port has been changed from 1/1 to 3/3


Verify running configuration with new primary port
==================================================

device(config-lag-test)# show running-config lag test
!
lag port-primary-dynamic
lag "test" dynamic id 10
 ports ethernet 1/1 to 1/4 ethernet 3/1 to 3/4
 primary-port 3/3
 deploy
!
!
!
```

The following example verifies that the primary port has changed from 1/1 to 1/2 while removing the existing primary port.

```
device(config-lag-test)# show running-configuration lag test
!
lag port-primary-dynamic
lag "test" dynamic id 10
 ports ethernet 1/1 to 1/4 ethernet 3/1 to 3/4
 primary-port 1/1
 deploy
!
!


Note: Remove existing primary port and the system selects primary port dynamically from existing ports
which has next available least port ID

device(config-lag-test)# no primary-port 1/1

SYSLOG: <14>Jul 18 16:26:52 LAG: test (id=10) , Configured primary port has been changed from 1/1 to 1/2

Verify running configuration with new primary port
==================================================

device(config-lag-test)# show running-config lag test
!
lag port-primary-dynamic
lag "test" dynamic id 10
 ports ethernet 1/1 to 1/4 ethernet 3/1 to 3/4
 primary-port 1/2
 deploy
!
!
!
```

The following example verifies that the primary port has changed from 1/1 to 1/2 when we remove the existing primary port from the LAG.

```
device(config-lag-test)# disable ethernet 1/1

SYSLOG: <14>Jul 18 16:52:22 System: Interface ethernet 1/1, state down - disabled

SYSLOG: <14>Jul 18 16:52:22 PORT: 1/1 disabled by operator from console session.
device(config-lag-test)#

device(config-lag-test)# no ports ethernet 1/1

SYSLOG: <14>Jul 18 16:52:37 LAG: test (id=10) , Configured primary port has been changed from 1/1 to 1/2

device(config-lag-test)# show running-configuration lag test

lag port-primary-dynamic
lag "test" dynamic id 10
ports ethernet 1/2 to 1/4 ethernet 3/1 to 3/4
primary-port 1/2
deploy
!
!
```

History

Release version	Command history
6.0.00a	This command was introduced.

pre-shared-key

Configures the pre-shared MACsec key on the interface.

Syntax

pre-shared-key *key-id* **key-name***name*

no pre-shared-key *key-id* **key-name***name*

Command Default

No pre-shared MACsec key is configured on the interface.

Parameters

key-id

Specifies the Connectivity Association Key (CAK) key value. Key-id must be hexadecimal string of 32 characters.

name

Specifies the Connectivity Association Key (CAK) key name. Key-name must be hexadecimal string of maximum 64 characters.

Modes

dot1x-mka-interface mode.

Usage Guidelines

The pre-shared key is required for communications between MACsec peers.

NOTE

1. Group must be attached to the interface before applying pre-shared key on the interface.
2. Key-name length should be multiple of 4.
3. Key-name and pre-shared key must be hexadecimal string.

The **no** form of the command removes the pre-shared key from the interface.

Examples

The following example configures pre-shared key with a name beginning with 11223344 and with the value shown, to port 1, slot 1 on the device.

```
device configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# enable-mka ethernet 1/1
device(config-dot1x-mka-eth-1/1)# pre-shared-key 0102030405060708090A0B0C0D0E0F10 key-name 11223344
```

History

Release version	Command history
5.8.00	This command was introduced.

pre-shared-key (IKEv2)

Configures a pre-shared key (PSK) for an Internet Key Exchange version 2 (IKEv2) authentication proposal.

Syntax

pre-shared-key { *string* | **hex-based** *hex-string* }

no pre-shared-key { *string* | **hex-based** *hex-string* }

Command Default

The default PSK is a text-based string; $QG5HTT1Ebk1TVW5NLWlhVW5ATVMhLS0rc1VA.

Parameters

string

Specifies a text-based PSK. The range is from 1 through 100 ASCII characters. Permitted values are:

- **Lower case letters:** a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z
- **Upper case letters:** A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
- **Number:** 1,2,3,4,5,6,7,8,9,0
- **Special Characters:** "!","@","#","$","%","^","&","*","(",")"
- **Additional special characters:** "", "{","}","[","]","-","_","=","+",";",":",",".","<",">","/","\?","|","`",

(To use "?", it must be preceded by "\", that is; "\?".)

hex-based *hex-string*

Specifies a hexadecimal-based PSK. The range is from 1 through 100 hexadecimal digits from the following set:

- 1,2,3,4,5,6,7,8,9,0,a,b,c,d,e,f,A,B,C,D,E,F.

Modes

IKEv2 auth-proposal configuration mode.

Usage Guidelines

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

Examples

The following example shows how to configure a text-based PSK for an IKEv2 authentication proposal named psk-example1.

```
device(config)# ikev2 auth-proposal psk-example1
device(config-ike-auth-psk-example1)# pre-shared-key
abcdefghijkmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ!@#$%^&*()
```

The following example shows how to configure a hexadecimal-based PSK for an IKEv2 authentication proposal named psk-example2.

```
device(config)# ikev2 auth-proposal psk-example2
device(config-ike-auth-psk-example2)# pre-shared-key hex-based 1234567890abcdef0987654321ABCDEF
```

preforwarding-time

Configures the preforwarding time interval, the time a port will remain in the preforwarding state before changing to the forwarding state.

Syntax

preforwarding-time *milliseconds*

no preforwarding-time *milliseconds*

Command Default

The default preforwarding time interval is 300 milliseconds.

Parameters

milliseconds

The preforwarding time interval in milliseconds. The range is from 200 through 30000 milliseconds.

Modes

MRP configuration mode

Usage Guidelines

The preforwarding time interval must be at least twice the value of the hello time or a multiple of the hello time.

When MRP is enabled, all ports begin in the preforwarding state.

An interface changes from the preforwarding state to the forwarding state when the port preforwarding time expires. This occurs if the port does not receive a Ring Health Packet (RHP) from the master, or if the forwarding bit in the RHPs received by the port is off (indicating a break in the ring). The port heals the ring by changing its state to forwarding. If a member port in the preforwarding state does not receive an RHP within the preforwarding time, the port assumes that a topology change has occurred and changes to the forwarding state.

The secondary port on the master node changes to the blocking state if it receives an RHP, but changes to the forwarding state if the port does not receive an RHP before the preforwarding time expires. A member node preforwarding interface also changes from preforwarding to forwarding if it receives an RHP whose forwarding bit is on.

If Unidirectional Link Detection (UDLD) is also enabled on the device, Brocade recommends that you set the MRP preforwarding time slightly higher than the default of 300 ms; for example, to 400 or 500 ms.

The **no** form of the command sets the preforwarding time interval to the default.

Examples

The following example shows how to configure the preforwarding time to 400 milliseconds.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)# preforwarding-time 400
```

prf

Configures a pseudorandom function (PRF) for an Internet Key Exchange version 2 (IKEv2) proposal.

Syntax

prf { **sha256** | **sha384** }

no prf { **sha256** | **sha384** }

Command Default

The default algorithm is SHA-384.

Parameters

sha256

Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.

sha384

Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.

Modes

IKEv2 proposal configuration mode

Usage Guidelines

This hash algorithm is used to generate key material during IKEv2 SA negotiations.

Both algorithms may be configured for an IKEv2 proposal.

When only one PRF algorithm is configured for an IKEv2 proposal, removing it restores the default configuration.

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

Examples

The following example shows how to configure SHA-256 as the hash algorithm for an IKEv2 proposal named ikev2_prop.

```
device(config)# ikev2 proposal ikev2_prop
device(config-ikev2-proposal-ikev2_prop)# prf sha256
```

History

Release version	Command history
05.8.00	This command was introduced.

protected

Configures VRF traffic protection for an Internet Key Exchange version 2 (IKEv2) profile.

Syntax

protected *vrf*

no protected *vrf*

Parameters

vrf

Specifies the name of the VRF to be protected.

Modes

IKEv2 profile configuration mode

Usage Guidelines

When the tunnel VRF and the protected VRF do not match, an IKEv2 session is not initiated.

The **no** form of the command removes the specified VRF traffic protection configuration for the IKEv2 profile.

Examples

The following example shows how to configure an IKEv2 profile named test to protect traffic for a VRF named red.

```
device(config)# ikev2 profile test
device(config-ikev2-profile-test)# protected red
```

History

Release version	Command history
05.8.00	This command was introduced.

radius-server host

Configures the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

radius-server host { *ipv4-address* | *host-name* | *ipv6-address*} [**auth-port** *port-num* [**acct-port** *port-num* [{ **accounting-only** | **authentication-only** | **default** } [**ssl- auth-port** *port-num* [**accounting-only** | **authentication-only** | **default**][**key** *key-string* [**dot1x**]]]]]

no radius-server host { *ipv4-address* | *host-name* | *ipv6-address*} [**auth-port** *port-num* [**acct-port** *port-num* [{ **accounting-only** | **authentication-only** | **default** } **ssl- auth-port** *port-num* [**accounting-only** | **authentication-only** | **default**] [**key** *key-string* [**dot1x**]]]]]

Command Default

The RADIUS server host is not configured.

Parameters

ipv4-address

Configures the IPv4 address of the RADIUS server.

host-name

Configures the host name of the RADIUS server.

ipv6-address

Configures the IPv6 address of the RADIUS server.

auth-port *port-num*

Configures the authentication UDP port. The default value is 1812.

acct-port *port-num*

Configures the accounting UDP port. The default value is 1813.

accounting-only

Configures the server to be used only for accounting.

authentication-only

Configures the server to be used only for authentication.

default

Configures the server to be used for any AAA operation.

key *key-string*

Configures the unique RADIUS key for the server.

dot1x

Configures support for EAP for 802.1X.

ssl-auth-port *port-num*

Specifies that the server is a RADIUS server running over a TLS-encrypted TCP session. Only one of auth-port or ssl-auth-port can be specified. If neither is specified, it defaults to the existing default behavior, which uses the default auth-port of 1812 and 1813 for accounting with no TLS encryption. The default destination port number for RADIUS

over TLS is TCP/2083.There are no separate ports for authentication, accounting, and dynamic authorization changes. The source port is arbitrary.

accounting-only
Configures the server to be used only for accounting.

authentication-only
Configures the server to be used only for authentication.

default
Configures the server to be used for any AAA operation.

Modes

Global configuration mode

Usage Guidelines

Use the **radius-server host** command to identify a RADIUS server to authenticate access to a Brocade device. You can specify up to eight servers. If you add multiple RADIUS authentication servers to the Brocade device, the device tries to reach them in the order you add them. To use a RADIUS server to authenticate access to a Brocade device, you must identify the server to the Brocade device. In a RADIUS configuration, you can designate a server to handle a specific AAA task. For example, you can designate one RADIUS server to handle authorization and another RADIUS server to handle accounting. You can specify individual servers for authentication and accounting, but not for authorization. You can set a unique RADIUS key for each server.

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

Examples

The following example shows how to configure a RADIUS server to authenticate access to a Brocade device.

```
device(config)# radius-server host 192.168.10.1
```

The following example shows how to specify different RADIUS servers for authentication and accounting.

```
device(config)# radius-server host 10.2.3.4 auth-port 1800 acct-port 1850 default key abc
device(config)# radius-server host 10.2.3.5 auth-port 1800 acct-port 1850 authentication-only key def
device(config)# radius-server host 10.2.3.6 auth-port 1800 acct-port 1850 accounting-only key ghi
```

The following example shows how to map the 802.1X port to a RADIUS server.

```
device(config)# radius-server host 10.2.3.4 auth-port 1800 acct-port 1850 default key abc dot1x
```

The following example shows how to specify different RADIUS servers for TLS authentication and accounting.

```
device(config)# radius-server host 10.2.3.4 ssl-auth-port 1800 default key abc
```

rate-limit exclude-ethernet-overhead

Enables the overhead exclusion for the rate limiting calculation (only if rate limiting is configured).

[rate-limit] exclude-ethernet-overhead

no [rate-limit] exclude-ethernet-overhead

QoS policy configuration mode

System statistics configuration mode

The command must be configured in both the QoS policy and system statistics modes.

In Q0S policy mode the command to enable exclusion of Ethernet overhead includes the term **rate-limit**, and is entered as **rate-limit exclude-ethernet-overhead**. However, when in system statistics mode, the command does not include the term **rate-limit**, and is entered as **exclude-ethernet-overhead**.

When enabled, this feature applies to all rate limit modes, on all supported modules, and affects all logical ports. If the command is not applicable to the unsupported module or slot, the configuration is ignored at the logical port.

Local port reload is not required.

.

The following configures the Ethernet overhead exclusion.

```
device# configure terminal
device(config)# qos-policy
device(config-qos-policy)# rate-limit exclude-ethernet-overhead
device(config-qos-policy)# exit
device(config)# statistics
device(config-statistics)# exclude-ethernet-overhead
```

The following example removes the Ethernet overhead exclusion configuration, both the QoS policy and system statistics contexts must be unset.

```
device# configure terminal
device(config)# qos-policy
device(config-qos-policy)# no rate-limit exclude-ethernet-overhead
device(config-qos-policy)# exit
device(config)# statistics
device(config-statistics)# no exclude-ethernet-overhead
```

Verification that the feature is configured, appears in the **show running-config** or **show startup-config** command output.

```
device# show running-config
(truncated output}
...
!
statistics
 exclude-ethernet-overhead
!
...(truncated output}
!
qos-policy
 rate-limit exclude-ethernet-overhead
!
...
(truncated output}
```

Release version	Command history
5.9.00a	This command was introduced.

rate-limit input

Configures incoming rate-limiting per port; or port per VLAN; or broadcast, unknown-unicast, or multicast (BUM) transmission methods. You can also rate-limit by applying an ACL.

Syntax

rate-limit input *average-rate maximum-burst*

rate-limit input [**vlan** *vlan-id*] { [**broadcast**] [**unknown-unicast**] [**multicast**] } *average-rate maximum-burst* [**include-control**] [**alert** *high-watermark low-watermark*] [**shutdown** [*timeout*]]

rate-limit input vlan *vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

rate-limit input access-group name { **ipv4** | **ipv6** | **mac** } *acl-name* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

rate-limit input vrf *vrf-name* **access-group name** { **ipv4** | **ipv6** } *acl-name* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

rate-limit input [**vrf** *vrf-name*] **access-group** *acl-num* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

rate-limit input mac *HHHH.HHHH.HHHH vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

rate-limit input group *vlan-group-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

no rate-limit input *average-rate maximum-burst*

no rate-limit input [**vlan** *vlan-id*] { [**broadcast**] [**unknown-unicast**] [**multicast**] } *average-rate maximum-burst* [**include-control**] [**alert** *high-watermark low-watermark*] [**shutdown** [*timeout*]]

no rate-limit input vlan *vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

no rate-limit input access-group name { **ipv4** | **ipv6** | **mac** } *acl-name* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

no rate-limit input vrf *vrf-name* **access-group name** { **ipv4** | **ipv6** } *acl-name* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

no rate-limit input [**vrf** *vrf-name*] **access-group** *acl-num* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

no rate-limit input mac *HHHH.HHHH.HHHH vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

no rate-limit input group *vlan-group-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* [**include-control**] | **policy-map** *map-name* }

Parameters

average-rate

Specifies the maximum number of bits a port is allowed to receive during a one-second interval—the sum of the broadcast, unknown-unicast, and multicast (BUM) rate limits. Values range from 0 through the line rate of the port. For Brocade NetIron MLX Series and Brocade NetIron XMR Series series, enter a multiple of 8,144 bps. Otherwise, the software adjusts the rate you entered down to the closest multiple.

maximum-burst

Specifies the maximum burst of traffic allowed by the port.

vlan *vlan-id*

Specifies the VLAN id of the port on which the rate-limiting of BUM traffic is accounted.

broadcast

Specifies broadcast packets.

unknown-unicast

Specifies unknown-unicast packets.

multicast

Specifies multicast packets.

include-control

Extends the BUM rate-limit to include ARP and other control packets.

alert *high-watermark low-watermark*

Generates alert messages if the rate exceeds or is less than these values, and shuts down the port if the rate exceeds the high limit.

shutdown *timeout*

(Optional) Configures the port to shut down if the amount of BUM traffic exceeds the pre-defined limit. Values range from 0 (default) through 1440 minutes. A value of 0 disables the port until it is manually re-enabled.

vrf *vrf-name*

(Only available for Layer 3 ACLs) Limits application of the specified ACL to the VRF that you specify.

access-group

Specifies an access control list (ACL).

name *acl-name*

Specifies a named ACL.

mac

Specifies a Layer 2 (MAC) ACL.

ipv4

Specifies an IPv4 ACL.

ipv6

Specifies an IPv6 ACL.

acl-num

Specifies a numbered ACL, as follows:

- Numbered standard IPv4 ACLs range from 1 through 99.
- Numbered extended IPv4 ACLs range from 100 through 199.

- Numbered Layer 2 (MAC) ACLs range from 400 through 499, but are not supported if a non-default VRF is specified.
- (Only for Brocade NetIron MLX Series and Brocade NetIron XMR Series) Numbered user-defined ACLs (UDAs) extend from 2000 through 2999.

priority *queue-numbers*
Specifies one or more of the supported priority queues, as follows:

- **q0**—internal priority 0 and 1
- **q1**—internal priority 2 and 3
- **q2**—internal priority 4 and 5
- **q3**—internal priority 6 and 7

policy-map *map-name*
Specifies a policy-map name.

mac *HHHH.HHHH.HHHH*
Specifies a source MAC-based rate limit.

group *vlan-group-id*
Species a VLAN Group ID to which the policy applies.

Modes

Interface configuration mode

Usage Guidelines

The maximum burst value cannot be more than the port line rate.

The highest permitted *maximum-burst* value varies with *average-rate*, as described in the following table:

TABLE 5 Maximum Burst Size

Average rate (bps)	Maximum burst size (Bits)
1 Mbps	66,535
1 - 10 Mbps	524,280
10 - 100 Mbps	4,194,240
100 Mbps - 1 Gbps	33,553,920
1 Gbps - 10 Gbps	268,431,230

If you specify more than one of the **broadcast**, **multicast**, or **unknown-unicast** keywords, the BUM rate limit that you define applies to the total for all of those transmission methods.

On a given port, you can specify up to 990 priority or 3960 non-priority rate-limit policies. (You can set the upper limit up to 3960 with the **qos-policy** command.)

When a VLAN-based traffic policing policy is applied to a port, all the ports controlled by the same packet processor are rate-limited for that VLAN. You cannot apply a VLAN-based traffic policing policy on another port of the same packet processor for that VLAN.

ACL types available for traffic filtering (as described in the *Brocade NetIron Security Configuration Guide*) are also available for rate limiting:

TABLE 6 ACL types by protocol

Protocol	Standard / Extended	Numbered / Named
MAC	Standard only	Numbered or Named
IPv4	Standard or Extended	Numbered or Named
IPv6	Standard or Extended	Named only
User-defined ACLs (UDAs)		(MLX/XMR series only) Numbered or Named

The **no** forms of this command cancel incoming rate limiting.

Examples

The following example is for rate-limit broadcast and multicast configuration.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input broadcast 100000 10000 include-control shutdown 1 alert
80000 10000
device(config-if-e1000-1/1)# rate-limit input multicast 100000 10000 include-control shutdown 1 alert
80000 10000
```

The following example is for a port-based and priority-based traffic policing policy.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input priority q1 500000000 33553920
```

The following example is for a port-and-VLAN based traffic policing policy.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input vlan 10 500000000 33553920
device(config)# interface ethernet 1/2
device(config-if-e1000-1/2)# rate-limit input vlan 20 policy-map map1
```

The following example is for rate-limit input ACL configuration, using numbered ACLs.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input access-group 400 100000 10000 include-control
device(config-if-e1000-1/1)# rate-limit input access-group 1 100000 10000 include-control
device(config-if-e1000-1/1)# rate-limit input access-group 100 100000 10000 include-control
```

The following example is for rate-limit input ACL configuration, using a named IPv4 ACL and a policy map.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input access-group name ipv4 ACG3001 policy-map INC3001
```

The following example configures rate-limiting for inbound IPv6 traffic using ACL “fdry”, setting the average rate as 1000000 and the maximum burst size as 2000000.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input access-group name ipv6 fdry 1000000 2000000
```

The following example configures rate-limiting for inbound IPv6 traffic using ACL “fdry” and the policy-map “map5”.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input access-group name ipv6 fdry policy-map map5 include-
control
```

The following example configures rate-limiting for inbound traffic on priority-queue “q0”, using the IPv6 access-list “fdry”, the average rate as 1000000 and the maximum burst size as 2000000.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input access-group name ipv6 fdry priority q0 1000000 2000000
```

The following example configures rate-limiting for inbound traffic on the VRF “data”, using the access-list “fdry”.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit input vrf data access-group name ipv6 fdry 1000000 2000000
include-control
```

History

Release version	Command history
05.7.00	This command was introduced.
05.9.00	This command was modified to support the **include-control** option.
06.1.00	This command was modified to support IPv6 ACLs and to support a non-default VRF option.

rate-limit output

Configures outgoing rate-limiting per port or port per VLAN. You can also rate-limit by applying an ACL.

Syntax

rate-limit output *average-rate maximum-burst*

rate-limit output [**vlan** *vlan-id*] *average-rate maximum-burst*

rate-limit output vlan *vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

rate-limit output access-group name { **ipv4** | **ipv6** | **mac** } *acl-name* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

rate-limit output access-group *acl-num* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

rate-limit output mac *HHHH.HHHH.HHHH vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

rate-limit output group *vlan-group-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

no rate-limit output *average-rate maximum-burst*

no rate-limit output [**vlan** *vlan-id*] *average-rate maximum-burst*

no rate-limit output vlan *vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

no rate-limit output access-group name { **ipv4** | **ipv6** | **mac** } *acl-name* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

no rate-limit output access-group *acl-num* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

no rate-limit output mac *HHHH.HHHH.HHHH vlan-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

no rate-limit output group *vlan-group-id* [**priority** *queue-numbers*] { *average-rate maximum-burst* | **policy-map** *map-name* }

Parameters

average-rate

Specifies the maximum number of bits a port is allowed to send during a one-second interval—the sum of the broadcast, unknown-unicast, and multicast (BUM) rate limits. Values range from 0 through the line rate of the port. For Brocade NetIron MLX Series and Brocade NetIron XMR Series series, enter a multiple of 8,144 bps. Otherwise, the software adjusts the rate you entered down to the closest multiple.

maximum-burst

Specifies the maximum burst of traffic allowed by the port.

vlan *vlan-id*

Specifies the VLAN id of the port on which the rate-limiting of BUM traffic is accounted.

access-group

Specifies an access control list (ACL).

name *acl-name*
Specifies a named ACL.

mac
Specifies a Layer 2 (MAC) ACL.

ipv4
Specifies an IPv4 ACL.

ipv6
Specifies an IPv6 ACL.

acl-num
Specifies a numbered ACL, as follows:

- Numbered standard IPv4 ACLs range from 1 through 99.
- Numbered extended IPv4 ACLs range from 100 through 199.
- Numbered Layer 2 (MAC) ACLs range from 400 through 499, but are not supported if a non-default VRF is specified.
- (Only for Brocade NetIron MLX Series and Brocade NetIron XMR Series) Numbered user-defined ACLs (UDAs) extend from 2000 through 2999.

priority *queue-numbers*
Specifies one or more of the supported priority queues, as follows:

- **q0**—internal priority 0 and 1
- **q1**—internal priority 2 and 3
- **q2**—internal priority 4 and 5
- **q3**—internal priority 6 and 7

policy-map *map-name*
Specifies a policy-map name.

mac *HHHH.HHHH.HHHH*
Specifies a source MAC-based rate limit.

group *vlan-group-id*
Species a VLAN Group ID to which the policy applies.

Modes

Interface configuration mode

Usage Guidelines

The maximum burst value cannot be more than the port line rate.

The highest permitted *maximum-burst* value varies with *average-rate*, as described in the following table:

TABLE 7 Maximum Burst Size

Average rate (bps)	Maximum burst size (Bits)
1 Mbps	66,535
1 - 10 Mbps	524,280

TABLE 7 Maximum Burst Size (continued)

Average rate (bps)	Maximum burst size (Bits)
10 - 100 Mbps	4,194,240
100 Mbps - 1 Gbps	33,553,920
1 Gbps - 10 Gbps	268,431,230

On a given port, you can specify up to 990 priority or 3960 non-priority rate-limit policies. (You can set the upper limit up to 3960 with the **qos-policy** command.)

When a VLAN-based traffic policing policy is applied to a port, all the ports controlled by the same packet processor are rate-limited for that VLAN. You cannot apply a VLAN-based traffic policing policy on another port of the same packet processor for that VLAN.

ACL types available for traffic filtering (as described in the *Brocade NetIron Security Configuration Guide*) are also available for rate limiting:

TABLE 8 ACL types by protocol

Protocol	Standard / Extended	Numbered / Named
MAC	Standard only	Numbered or Named
IPv4	Standard or Extended	Numbered or Named
IPv6	Standard or Extended	Named only
User-defined ACLs (UDAs)		(MLX/XMR series only) Numbered or Named

The **no** forms of this command cancel outgoing rate limiting.

Examples

The following example is for a port-based and priority-based traffic policing policy.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-1/1)# rate-limit output priority q1 500000000 33553920
```

The following example is for a port-and-VLAN based traffic policing policy.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-1/1)# rate-limit output vlan 10 500000000 33553920
device(config)# interface ethernet 1/2
device(config-if-1/2)# rate-limit output vlan 20 policy-map map1
```

The following example is for rate-limit output ACL configuration.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit output access-group 400 100000 10000
device(config-if-e1000-1/1)# rate-limit output access-group 1 100000 10000
device(config-if-e1000-1/1)# rate-limit output access-group 100 100000 10000
```

The following example configures rate-limiting for outbound traffic using the IPv6 access-list “outrate_1”, the average rate as 1000000 and the maximum burst size as 2000000.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit output access-group name ipv6 outrate_1 1000000 2000000
```

The following example configures rate-limiting for outbound traffic using the IPv6 access-list “outrate_1” and the policy-map “map6”.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit output access-group name ipv6 outrate_1 policy-map map6
```

The following example configures rate-limiting for outbound traffic on priority-queue “q0” using the IPv6 access-list “outrate_1”, the average rate as 1000000 and the maximum burst size as 2000000.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit output access-group name ipv6 outrate_1 priority q0 1000000
2000000
```

History

Release version	Command history
06.1.00	This command was modified to support IPv6 ACLs.

rate-limit strict-acl

Configures an interface to drop packets that match a deny rule or do not match any rule in an ACL applied for rate limiting.

Syntax

rate-limit strict-acl

no rate-limit strict-acl

Command Default

The strict ACL option is disabled. Packets that do not match any ACL rule or match a deny rule, are forwarded normally (neither dropped nor rate-limited).

Modes

Interface configuration mode

Usage Guidelines

Strict ACL applies to Layer-2 ACLs, IPv4 ACLs, IPv6 ACLs, and user-defined ACLs (UDA) for rate-limiting on that interface.

The **no** form of this command disables the **rate-limit strict-acl** feature.

Examples

The following example enables strict ACL rate-limiting on an interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# rate-limit strict-acl
```

rd

Each instance of a VRF must have a unique Route Distinguisher (RD) assign to it.

Syntax

rd { *as-num:id* | *ip-num:id* }

no rd { *as-num:id* | *ip-num:id* }

Command Default

No RD is assigned to the VRF.

Parameters

as-num:id

Composed of the local ASN number followed by a colon ":" and a unique arbitrary number. For example 3:6.

ip-num:id

Composed of the local IP address followed by a colon ":" and a unique arbitrary number.

Modes

VRF configuration mode

Usage Guidelines

Each instance of a VRF must have a unique Route Distinguisher (RD) assigned to it. The RD is pre-pended to any address being routed or advertised. The RD can be defined as either ASN relative or IP address relative. Because the RD is unique to an instance of a VRF, it allows the same IP address to be used in different VPNs without creating any conflict.

The **no** form of the command returns to the default setting.

Examples

The following example displays the command which assigns a Route Distinguisher (RD) based on the AS number 3 and the arbitrary identification number 6.

```
device(config-vrf)# rd 3:6
```

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* | **route-map** *string*]

redistribute { *source-protocol* } [**metric** *num* | **metric-type** { **type1** | **type2** } | **route-map** *string*]

redistribute { **isis** } [**level-1** | **level-1-2** | **level-2** | **metric** *num* | **metric-type** { **type1** | **type2** } | **route-map** *string*]

no redistribute { **ospf** } [**match** [**external1** | **external2** | **internal**]] [**metric** *num*] [**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.

source-protocol

Specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **isis**, **ospf**, **rip**, or **static**.

metric *num*

Specifies a metric for redistributed routes. Range is from 0 through 65535. No value is assigned by default.

route-map *string*

Specifies a route map to be consulted before a route is added to the routing table.

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.

level-1

Specifies level-1 routes.

level-1-2
Specifies both level-1 and level-2 routes.

level-2
Specifies level-2 routes.

Modes

BGP 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 configuration mode and OSPFv3 router VRF configuration mode.

[**match metricmetric-type**

NOTE
The **default-metric** command does not apply to the redistribution of directly connected routes. Use a route map to change the default metric for directly connected routes.

The **no** form of the command restores the defaults.

The **level-1** , **level-1-2** , and **level-2** options are only available if the **isis** keyword is entered.

NOTE
Prior to software release 04.1.00, the **redistribution** command is used instead of the **redistribute** command

Examples

The following example redistributes OSPF external type 1 routes.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# redistribute ospf match external1
```

The following example redistributes OSPF routes with a metric of 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# redistribute ospf metric 200
```

The following example redistributes OSPFv3 external type 2 routes in VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# 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)# address-family ipv6 unicast
device(config-bgp-ipv6u)# redistribute static metric 200
```

The following example redistributes IS-IS routes into BGP4+ in VRF instance "red".

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

The following example redistributes RIP routes and specifies that route-map "rm2" be consulted in BGP address-family IPv6 unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast
device(config-bgp-ipv6u)# redistribute rip route-map rm2
```

The following example redistributes BGP routes and specifies that route-map "rm7" be consulted in OSPF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# 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-ospf6-router)# redistribute ospf metric-type type1
```

The following example redistributes IS-IS level-1 and level-2 routes in OSPFv3 VRF configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# redistribute isis level-1-2
```

remove-tagged-ports / remove-untagged-ports

Removes tagged or untagged ports on the VLAN.

Syntax

remove-tagged-ports

remove-untagged-ports

Command Default

None.

Modes

VLAN configuration mode (config-vlan).

Examples

The following example displays the remove-tagged-ports command.

```
device(config-vlan-100)# remove-tagged-ports
Vlan : 100, Ports removed : ethe 1/1 to 1/2 ethe 4/1 to 4/8
device(config-vlan-100)#
```

The following example displays the remove-untagged-ports command.

```
device(config-vlan-100)# remove-untagged-ports
Vlan : 100, Ports removed : ethe 3/1 to 3/24
device(config-vlan-100)#
```

History

Release version	Command history
5.8.00	This command is introduced.

remove-vlan

Removes tagged and untagged ports from all or defined VLANs.

Syntax

remove-vlan [**all** | **vlan** [*vlan_id*]] { **to** *vlan_id* }

Parameters

all

Removes all configured VLANs.

vlan *vlan_id*

Specifies the VLAN where the ports should be removed.

to *vlan_id*

Specifies the VLAN range to remove.

Modes

User configuration level.

Examples

The following example displays the command with the **all** option.

```
device(config-if-e100000-1/1)# remove-vlan all
Port ethe 1/1  removed from tagged vlan : 300 400 500 600 700 800 900 1000 2000 3000 4000  and untagged
vlan : 200 .
device(config-if-e100000-1/1)#
```

The following example displays the command with a specified VLAN range.

```
device(config-if-e100000-1/2)# remove-vlan vlan 2 to 4090
Port ethe 1/2  removed from tagged vlan : 300 400 500 600 700 800 900 1000 2000 3000 4000  and untagged
vlan : 200 .
device(config-if-e100000-1/2)#
```

The following example displays the command that remove a specific VLAN.

```
device(config-if-e10000-4/1)# remove-vlan vlan 500
Vlan : 500, Ports removed : ethe 4/1
device(config-if-e10000-4/1)#
```

History

Release version	Command history
5.8.00	This command was introduced.

restart-ports

Configures a VSRP-configured device to shut down its ports when a failover occurs and restart after a period of time.

Syntax

restart-ports [*seconds*]

no restart-ports *seconds*

Command Default

The default is 1 second.

Parameters

seconds

Specifies the time the VSRP master shuts down its port before it restarts. The range is from 1 through 120 seconds.

Modes

VSRP VRID configuration mode

Usage Guidelines

The VSRP fast start feature can be enabled on a VSRP-configured Brocade device, either on the VLAN to which the VRID of the VSRP-configured device belongs (globally) or on a port that belongs to the VRID. This command shuts down all the ports that belong to the VLAN when a failover occurs. All the ports will have the specified VRID.

The **no** form of the command resets the time to the default.

Examples

The following example configures the ports to restart in 5 seconds.

```
device(config)# vlan 100
device(config-vlan-100)# vsrp vrid 1
device(config-vlan-100-vrid-1)# restart-ports 5
```

retransmit-interval

Sets the time the device waits before it retransmits Link State PDUs (LSPs).

Syntax

retransmit-interval *interval*

retransmit-interval *interval*

Command Default

The default retransmission interval is 5 seconds.

Parameters

secs

Specifies the retransmission interval in seconds. Valid values range from 1 through 65535 seconds. The default is 5 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command removes the configured interval.

Examples

The following example changes the retransmission interval to 7 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# retransmit-interval 7
```

reverse-metric

Configures the reverse metric value at the Intermediate System-to-Intermediate System (IS-IS) router level.

Syntax

reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

reverse-metric tlv-type [*value*]

no reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

no reverse-metric tlv-type [*value*]

Command Default

The **reverse-metric** command is disabled by default.

Parameters

reverse-metric	Specifies the reverse metric parameter at the IS-IS router level.
value	Specifies the reverse metric value in metric style. The metric style consists of narrow or wide style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default value is 16777214 irrespective of the metric style configured.
te-def-metric	Specifies that the device sends a traffic engineering (TE) default metric sub-type-length-value (TLV) within the reverse-metric TLV.
whole-lan	Specifies that the configured reverse metric value affects the entire LAN.
tlv-type *value*	Specifies the TLV type for the reverse metric value. The default value is 254.

Modes

IS-IS router configuration mode

Usage Guidelines

If the reverse-metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor device receives the reverse metric value through the IS hello, the neighbor router updates the cost to reach the original IS-IS router with the sum of default metric and the reverse metric value.

The **whole-lan** option only takes effect on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the **whole-lan** option is used.

The **no** form of the command specified with the configured value resets the metric value to the default value of 16777214. The **no reverse-metric** command removes the entire reverse metric configuration.

NOTE

The **reverse-metric** *value* command is supported on the Brocade NetIron XMR Series, the Brocade MLX Series, and the Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

Examples

The following example changes the reverse metric value for the entire LAN to 50.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# reverse-metric 50 whole-lan
```

The following example configures the reverse metric TLV type in the range of unassigned IS-IS TLV values.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# reverse-metric tlv-type 230
```

History

Release version	Command history
5.7.00	This command was introduced.

revocation-check

Specifies the type of method to be followed for revocation check of the certificate authority (CA).

Syntax

revocation-check { **crl** | **ocsp** | **none** }

no revocation-check { **crl** | **ocsp** | **none** }

Command Default

Revocation check is not enabled.

Parameters

crl

Specifies the certificate revocation list (CRL) method for revocation check.

ocsp

Specifies the Online Certificate Status Protocol (OCSP) method for revocation check.

none

Specifies that none of the methods are selected for revocation check.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The **no** form of the command removes the method selected for revocation check.

Examples

The following example specifies the crl as the revocation check method.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# revocation-check crl
```

History

Release version	Command history
5.9.00	This command was introduced.

rfc1583-compatibility (OSPF)

Configures compatibility with RFC 1583.

Syntax

rfc1583-compatibility

no rfc1583-compatibility

Command Default

This command is disabled by default.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Enter **no rfc1583-compatibility** to disable compatibility with RFC 1583 if it has been enabled. Enter **no rfc1583-compatibility** if it has been enabled to re-enable compatibility with RFC 2328.

When this command is enabled, OSPF is compatible with RFC 1583 (OSPFv2) and OSPF prefers the least cost path to the autonomous system border router (ASBR). Disabling this compatibility causes OSPF to prefer the non-backbone area path over backbone area paths in addition to the least cost path to the ASBR.

When upgrading software from 5.8x and earlier, the device preserves the existing configuration value for OSPF RFC 1583 compatibility based on the version of the startup configuration file. New OSPF configurations use the new default value.

Examples

This example enables compatibility with RFC 1583.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# rfc1583-compatibility
```

This example disables compatibility with RFC 1583 if it has been enabled and re-enables compatibility with RFC 2328.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# no rfc1583-compatibility
```

History

Release version	Command history
5.9.00	This command was modified so that it is disabled by default.

Release version	Command history
5.9.00a	This command was modified so that existing configurations are preserved when upgrading software.

ring-interface

Configures the primary and secondary interfaces for the ring to control outward traffic flow.

Syntax

ring-interface ethernet *slot/port* **ethernet** *slot/port*

no ring-interface ethernet *slot/port* **ethernet** *slot/port*

Command Default

The primary and secondary interfaces are not configured.

Parameters

ethernet *slot/port*

Configures the primary and secondary interfaces.

Modes

MRP configuration mode

Usage Guidelines

On the master node, the primary interface is the one that originates Ring Health Packets (RHPs). Ring control traffic and Layer 2 data traffic will flow in the outward direction from this interface by default. On member nodes, the direction of traffic flow depends on the traffic direction selected by the master node. Therefore, on a member node, the order in which you enter the interfaces does not matter.

NOTE
The Brocade NetIron CES and CER Series devices do not support selection of a secondary interface based on reception of RHPs. As a result, the primary and secondary interfaces must be configured correctly.

The **no** form of the command clears the primary and secondary interfaces.

Examples

The following example shows how to configure the primary and secondary interfaces on a ring.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-2)# ring-interface ethernet 1/1 ethernet 1/2
```

router-interface

Configures the VE per VPLS instance.

Syntax

router-interface { **ve** *num* }

Command Default

None.

Parameters

ve *num*

Specifies the Virtual Ethernet interface number.

Modes

MPLS VPLS sub-configuration mode (config-mpls-vpls).

Usage Guidelines

The user must specify a router-interface for each VPLS instance.

Examples

The following example displays when the user must specify a router-interface for each VPLS instance.

```
device(config)# router mpls
device(config-mpls)# vpls test 10
device(config-mpls-vpls-test)# router-interface ve 200
device(config-mpls-vpls-test)# vlan 10
device(config-mpls-vpls-test-vlan-10)# tagged ethe 4/1
device(config-mpls-vpls-test-vlan-10)# vlan 200 isid 20000
```

router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing.

Syntax

router isis

Command Default

Disabled

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables IS-IS routing.

Examples

The following example enables IS-IS routing.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)#
```

router mpls

Enables MPLS and accesses MPLS configuration mode

Syntax

router mpls

no router mpls

Command Default

MPLS is disabled by default.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable MPLS on the device.

Examples

The following example enables MPLS on the device and access MPLS configuration mode.

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

router ospf

Enables and configures the Open Shortest Path First version 2 (OSPFv2) routing protocol.

Syntax

router ospf [**vrf** *name*]

no router ospf

Command Default

Disabled.

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-ospf-router)#
```

router vrrp

Globally enables Virtual Router Redundancy Protocol (VRRP).

Syntax

router vrrp

no router vrrp

Command Default

VRRP is not globally enabled.

Modes

Global configuration mode

Usage Guidelines

After globally enabling VRRP, the command prompt does not change. Nearly all subsequent VRRP configuration is performed at the interface level, but VRRP must be enabled globally before configuring VRRP instances.

The **no router vrrp** command disables VRRP globally.

Examples

The following example globally enables VRRP and enters interface configuration mode.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/5
```

router vsrp

Enables the Virtual Switch Redundancy Protocol (VSRP) on Layer 2 or Layer 3 switches.

Syntax

router vsrp

no router vsrp

Command Default

By default, VSRP is enabled on Layer 2 and Layer 3 switches.

Modes

Global configuration mode

Usage Guidelines

On a Layer 3 switch, if you want to use VRRP or VRRP-E for Layer 3 redundancy instead of VSRP, you must disable VSRP first. Because VRRP and VRRP-E do not apply to Layer 2 switches, there is no need to disable VSRP and there is no command to do so. VSRP is always enabled on Layer 2 switches.

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

Examples

The following example shows how to disable VSRP and then enable it.

```
device(config)# no router vsrp
device(config)# router vsrp
```

router vrrp-extended

Globally enables Virtual Router Redundancy Protocol Extended (VRRP-E) and enters VRRP-E router configuration mode.

Syntax

router vrrp-extended

no router vrrp-extended

Command Default

VRRP-E is not globally enabled.

Modes

Global configuration mode

Usage Guidelines

After globally enabling VRRP-E, nearly all subsequent VRRP-E configuration is performed at the interface level. VRRP-E must be enabled globally before configuring VRRP-E instances.

The **no router vrrp-extended** command globally disables VRRP-E.

Examples

The following example globally enables VRRP-E and enters interface configuration mode.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.3/24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 1
device(config-if-e1000-1/5-vrid-1)# backup priority 110
device(config-if-e1000-1/5-vrid-1)# version 2
device(config-if-e1000-1/5-vrid-1)# ip-address 10.53.5.254
device(config-if-e1000-1/5-vrid-1)# activate
VRRP-E router 1 for this interface is activating
```

rpf shortcut

Enables RPF shortcut for LSP paths.

Syntax

rpf shortcut

no rpf shortcut

Parameters

slot/port Specifies the port that you want to display RPF shortcuts for LSP paths.

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

When RPF lookup results in the LSP path, then another lookup is executed to get the underlying native route and that route's next-hop is used as the RPF.

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

Examples

To configure **rpf shortcut**, use this command in the configuration mode.

```
device(config)# router pim
device(config-pim-router)# rpf shortcut
```

History

Release	Command History
5.5.00	This command was modified to RPF shortcut for LSP paths information.

rsvp

Accesses MPLS RSVP configuration mode to configure RSVP-TE Hello.

Syntax

rsvp

no rsvp

Command Default

None

Modes

MPLS configuration mode

Usage Guidelines

Use the **no** form to remove the RSVP-TE Hello configuration globally.

Use the **no** form to remove RSVP-TE Hello configuration globally or on the MPLS interface.

Examples

The following example accesses MPLS RSVP configuration mode to configure RSVP-TE Hello globally.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# rsvp
device(config-mpls-rsvp)#
```

rsvp-hello

Configures the RSVP-TE Hello with default values on all the mpls-interfaces, providing the mpls-interface does not have any local-interface level configuration for the same.

Syntax

rsvp-hello [**acknowledgments** [**interval** *num* | **tolerance** *num*] | **interval** *num* | **tolerance** *num*]

no rsvp-hello [**acknowledgments** [**interval** *num* | **tolerance** *num*] | **interval** *num* | **tolerance** *num*]

Parameters

acknowledgments

Acknowledges RSVP Hellos on the interface supporting RSVP Hello and *not* having RSVP sessions.

interval *num*

Interval between two RSVP Hello requests in seconds. Value range is 1 - 60, default 9.

tolerance *num*

Number of unacknowledged RSVP Hello requests, seconds, before a timeout. Value range is 1 - 255, default 3.

Modes

MPLS configuration mode.

MPLS interface configuration mode.

Usage Guidelines

RSVP Hello configuration at the global MPLS RSVP level

Interval and tolerance for RSVP-TE Hello protocol can be configured at global MPLS RSVP level. The global configuration is pushed to all the mpls-interfaces when the interface level configurations are not present. In addition to these two parameters, one more parameter may be configured at global MPLS RSVP level, namely, acknowledgments.

Hello-interval and hello-tolerance at mpls-interface level

RSVP-TE Hello interval and tolerance can be configured at mpls-interface level as well. Interface level configurations take precedence over global configurations. These parameters can be individually configured for each mpls-interface.

By default, acknowledgments are *not sent* on mpls-interface supporting RSVP Hello when no sessions are taking that interface.

Interface-level configuration takes precedence over global configuration.

CAUTION
When disabling RSVP hello, disable it on both sides of the link at the same time to avoid bringing down all the RSVP sessions going over that link.

The **no** form of the command does not take interval or tolerance as parameters. Executing the **no rsvp-hello** command on the mpls-interface level sets the RSVP-TE Hello parameters to the globally configured RSVP Hello parameter values. If RSVP

Hello is not configured globally, it disables the RSVP Hello on the mpls-interface. Executing this removes the configuration from the interface level and will no longer display the RSVP Hello configuration at the interface level in the **show configuration** output.

Examples

The following example displays the command in the Global configuration mode.

```
device configure terminal
device(config)# router mpls
device(config-mpls)#rsvp
device(config-mpls-rsvp) rsvp-hello
device(config-mpls-rsvp) rsvp-hello interval 15 tolerance 5 acknowledgments
```

The following example displays the command in the Interface configuration mode.

```
device configure terminal
device(config)# router mpls
device(config-mpls-if-e100-1/1)# rsvp
device(config-mpls-if-e100-1/12) rsvp-hello
device(config-mpls-if-e100-1/12) rsvp-hello interval 5 tolerance 2
```

History

Release	Command history
5.6.00	The command was introduced.

rsvp-hello acknowledgments

Configures the RSVP-TE Hello to respond back with Hello ACKs to neighbors not carrying any RSVP sessions.

The **rsvp-hello acknowledgments** command configures the RSVP-TE Hello to respond back with Hello ACKs to neighbors not carrying any RSVP sessions. The configuring for acknowledgments is at the global MPLS RSVP level.

Syntax

rsvp-hello acknowledgments

no rsvp-hello acknowledgments

Modes

MPLS RSVP Hello global configuration mode.

Usage Guidelines

By default, RSVP-TE Hello does not send ACKs to neighbors not carrying any RSVP sessions.

The **no** format of this command sets it back to the default behavior of not sending ACKs to neighbors not carrying any RSVP sessions. This erases the configuration line from the global configuration. All the mpls-interfaces supporting RSVP Hello having *ZERO* sessions to neighbors *do not send HELLO_ACKs* for requests sent to those neighbors (which is the default behavior).

Examples

The following example enables RSVP-TE Hello on all mpls-interfaces with default values for hello-interval and hello-tolerance if no interface level specific configuration is present.

```
device configure terminal
device(config)# router mpls
device(config-mpls)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15
device(config-mpls-rsvp)# rsvp-hello tolerance 5
```

History

Release	Command history
5.6.00	This command was introduced.

rsvp-hello disable

Disables RSVP Hello on an mpls-interface.

Syntax

rsvp-hello disable

no rsvp-hello disable

Modes

MPLS interface configuration mode.

Usage Guidelines

This command erases the configuration line from the configuration like any other **no** command. When there is global configuration, the interface starts picking up globally configured parameters for the RSVP Hello.

If there is no global configuration, the interface does not run RSVP-Hello.

CAUTION
When disabling RSVP hello, please disable it on both sides of the link at the same time to avoid bringing down all the RSVP sessions going over that link.

The **no** form of the rsvp-hello command will not take any parameters other than **disable** at the interface level local configuration. When the parameter needs to be changed to the default value, the user has to execute the normal configuration command.

Examples

The following example displays the command under the Interface configuration.

```
device (config-mpls-if-e100-1/6)# rsvp-hello disable
```

The following example displays the RSVP Hello is being disabled on the interface. It generates on the configuration. The RSVP Hello would not be running on this interface irrespective of any global or local configuration present.

```
device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2

device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgements

device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2

device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/3

device(config-mpls-rsvp)# mpls-interface e1/4
device(config-mpls-rsvp)# rsvp-hello interval 20 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/5
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 7

device(config-mpls-rsvp)# mpls-interface e1/6
device(config-mpls-rsvp)# rsvp-hello disable
```

The following example displays that the RSVP Hello is configured with the default parameters on the interface. The parameters are auto-generated.

```
device (config-mpls-if-e100-1/7) rsvp-hello
device (config-mpls-if-e100-1/7) rsvp-hello disable

device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2

device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgements

device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2

device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/3

device(config-mpls-rsvp)# mpls-interface e1/4
device(config-mpls-rsvp)# rsvp-hello interval 20 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/5
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 7

device(config-mpls-rsvp)# mpls-interface e1/6
device(config-mpls-rsvp)# rsvp-hello disable

device(config-mpls-rsvp)# mpls-interface e1/7
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3
device(config-mpls-rsvp)# rsvp-hello disable
```

The following example displays that the RSVP Hello is enabled back on the interface. The interface starts taking the values that were previously configured on it. When there is no previous interface-specific configuration, then the interface starts taking all of the configuration from the Global level.

When there is no Global configuration as well, then the interface does not run RSVP Hellos.

```
device (config-mpls-if-e100-1/7) no rsvp-hello disable

device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2

device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgements

device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2

device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/3

device(config-mpls-rsvp)# mpls-interface e1/4
device(config-mpls-rsvp)# rsvp-hello interval 20 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/5
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 7

device(config-mpls-rsvp)# mpls-interface e1/6
device(config-mpls-rsvp)# rsvp-hello disable

device(config-mpls-rsvp)# mpls-interface e1/7
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3
```

The following example displays that the RSVP Hello's are being enabled back on the interface.

```
device (config-mpls-if-e100-1/6) no rsvp-hello disable Interval is 15 seconds (Global configuration).


device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2

device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgments

device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2

device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/3

device(config-mpls-rsvp)# mpls-interface e1/4
device(config-mpls-rsvp)# rsvp-hello interval 20 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/5
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 7

device(config-mpls-rsvp)# mpls-interface e1/6

device(config-mpls-rsvp)# mpls-interface e1/7
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3
```

History

Release	Command history
5.6.00	This command was introduced.

rx-label-silence-time

Defines the length of the receive label silence timer for for LDP-IGP synchronization.

Syntax

rx-label-silence-time *milliseconds*

no rx-label-silence-time

Command Default

The default value is 1000 milliseconds.

Parameters

milliseconds

Specifies the length of time in milliseconds of the receive label silence timer. Enter an integer from 100 to 60000.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default value of 1000 milliseconds.

When labels are not received from the peer for a short period of time, the session is declared In Sync. When a label is received from a peer, then the receive label silence timer is reset.

Examples

The following example sets the length of time for the receive label silence timer to 80000 milliseconds.

```
device(conf)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# rx-label-silence-time 80000
```

sample-recording

Use this command to set the sample recording for the LSP.

Syntax

sample-recording [**enable** | **disable**]

no sample-recording [**enable** | **disable**]

Command Default

Sample-recording is disabled.

Parameters

enable

Enables sample recording for the LSP.

disable

Disables sample recording for the LSP.

Modes

MPLS autobw-template configuration mode.

MPLS LSP mode.

Usage Guidelines

Under the MPLS LSP mode, when autobw-template is configured for this LSP, the sample recording configuration from the template is taken, otherwise sample recording is disabled by default.

This command configures the template to record the sample history.

Under the MPLS autobw-template config mode, the **no** option disables this option.

Examples

The following example shows when the the user wants to record the sample history for an LSP or template.

```
device configure terminal
device(config)# router mpls
device(config-mpls)# autobw-template template1
device(config-mpls-autobw-template-template1)# sample-recording enable


device configure terminal
device(config)# router mpls
device(config-mpls)# lsp lsp1-autobw
device(config-mpls-lsp-lsp1-autobw)# sample-recording enable
```

History

Release version	Command history
5.6.00	This command was introduced.

scale-timer

Configures a scale time factor that increases the timing sensitivity across all configured and default Virtual Router Redundancy Protocol Extended (VRRP-E) timers.

Syntax

scale-timer vrrp-extended *scale-factor*

no scale-timer vrrp-extended *scale-factor*

Command Default

VRRP timers are not scaled.

Parameters

vrrp-extended

A scale time factor can be configured for VRRP-E timers.

scale-factor

A number representing the scale of the division of a VRRP-E configured interval timer or the default interval timer. Valid values are in a range from 1 through 10. The default value is 1.

Modes

VRRP-E router configuration mode

Usage Guidelines

Configuring the VRRP-E scale timer is supported only in VRRP-E sessions. When a scaling value is configured, the existing timer values are divided by the scaling value. For example: a value of 10 divides the timers by a factor of 10, allowing the default dead interval to be set to 300 ms. Using timer scaling, VRRP-E subsecond convergence is possible if a master VRRP device fails.

NOTE

Increased timing sensitivity as a result of this configuration could cause protocol flapping during periods of network congestion.

NOTE

Brocade MLX devices only support a scaling factor of 10. For interoperability with MLX devices, use an advertisement interval scale factor of 10.

Examples

The following example scales all VRRP-E timers by a factor of 10.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# scale-timer vrrp-extended 10
```

scale-timer mrp

Decreases the Metro Ring Protocol (MRP) convergence time by changing the MRP scale timer value from 100 ms to 50 ms.

Syntax

scale-timer mrp

no scale-timer mrp

Command Default

The default MRP timer value is 50 ms.

Modes

Global configuration mode

Usage Guidelines

The effect of setting the scale timer is that the time taken to move from blocking to preforwarding and preforwarding to forwarding is (preforwarding value - the hello time). This is a significant change to the operation of MRP in the default state which has been described in the previous section.

NOTE
When setting the timer using the command, the actual value used will be exactly half of the input value.

The **no** form of the command changes the MRP timer tick value to 50 ms.

Examples

The following example decreases the MRP scale timer value from 100 ms to 50 ms.

```
device(config)# scale-timer mrp
```

scp

Copies a license file from an SCP-enabled client to the license database of the device.

Syntax

scp *license_file_on_hostuser@IP_address:* **license**

Command Default

By default, the command is not enabled.

Parameters

license_file_on_hostuser@IP_address:

Specifies the filename of the license file at the specified IP address.

license

Specifies the keyword license to be used.

Examples

The following example copies the license file from an SCP-enabled client to the license database.

```
device# scp license.xml terry@10.20.91.39:license
```

History

Release version	Command history
07.2.00	This command was introduced.
05.0.00	This command was introduced.

session

Configures an LDP session for the neighbor-based filtering of inbound or outbound FECs, You can also configure an authentication key for the LDP session.

Syntax

session *remote-ip-addr* { **filter-fec** *prefix-list* **in out** } | { **key** *string* }

no session *remote-ip-addr* { **filter-fec** *prefix-list* **in out** } | { **key** *string* }

Command Default

None

Parameters

remote-ip-addr

Specifies the IP address of the LDP peer.

filter-fec

Configures neighbor-based LDP FEC filtering.

prefix-list

Specifies the prefix list for the neighbor to which the filter is applied to allow or prevent the advertisement of FECs.

in

Applies filtering on inbound FECs.

out

Applies filtering on outbound FECs.

key *string*

Configures an authentication key on the LDP session. The LDP session can be to an adjacent peer (basic discovery) or to the targeted peer (extended discovery).The string variable specifies a text string of up to 80 characters used for authentication between LDP peers. It must be configured on both peers.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of the command to remove the neighbor-based FEC filtering or authentication key from the LDP session.

Examples

The following example configures LDP to prevent the advertisement of FEC 10.40.40.0/24 through the list-out prefix list and allow all others FECs to neighbor 10.12.12.12.

```
device# configure terminal
device(config)# ip prefix-list list-out deny 10.40.40.0/24
device(config)# ip prefix-list list-out permit 0.0.0.0/0 ge 32
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# session 10.12.12.12 filter-fec list-out out
```

set-debug

Enables debug configurations for Intermediate System-to-Intermediate System (IS-IS).

Syntax

set-debug nsr

no set-debug nsr

Command Default

Disabled.

Parameters

nsr	Specifies nonstop routing (NSR) debugs.

Modes

IS-IS router configuration mode

Examples

The following example enables NSR debug configurations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-debug nsr
```

The following example disables NSR debug configurations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no set-debug nsr
```

set-overload-bit

Configures a device to signal other devices not to use it as an intermediate hop in their shortest path first (SPF) calculations if the resources of the intermediate system are overloaded and preventing the IS from properly performing Intermediate System-to-Intermediate System (IS-IS) routing.

Syntax

set-overload-bit

set-overload-bit on-startup *value*

set-overload-bit on-startup wait-for-bgp [*max-bgp-wait-time*]

no set-overload-bit

no set-overload-bit on-startup *interval*

no set-overload-bit on-startup wait-for-bgp [*max-bgp-wait-time*]

Command Default

A device automatically sets the overload on in its Link State PDUs (LSPs) to other intermediate systems if an overload condition occurs.

Parameters

on-startup

Sets the overload bit when the system starts up. The overload bit remains set for the number of seconds configured or until Border Gateway Protocol (BGP) has converged, depending on the subsequent argument or keyword specified.

interval

Specifies the number of seconds the overload bit remains set when the system starts up. Valid values range from 5 through 86400 seconds (24 hours).

wait-for-bgp

Specifies that the overload bit is set when the system starts up and remains set until BGP has converged.

max-bgp-wait-time

Specifies the maximum time in seconds that IS-IS waits for BGP convergence to complete. When the configured time interval is exceeded without BGP convergence, IS-IS exits the overload state. Valid values range from 5 seconds through 86400 seconds (24 hours). The default is 600 seconds (10 minutes).

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command removes the configured overload state.

Examples

The following example sets the overload bit to on with immediate effect.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit
```

The following example configures the device to set the overload bit on in all its IS-IS LSPs sent to other ISs during the first five seconds following a successful software reload. After the five seconds expire, the device resets the overload bit to off in all its IS-IS LSPs.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit on-startup 60
```

The following example specifies that the overload bit is set upon system startup and remains set until BGP has converged and specifies that the device that 240 seconds is the maximum time that IS-IS will wait for BGP convergence to complete.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit on-startup wait-for-bgp 240
```

set next-hop-ip-tunnel

Configures a GRE tunnel interface as the next hop of a PBR route map.

Syntax

set next-hop-ip-tunnel *tunnel-id*

no set next-hop-ip-tunnel *tunnel-id*

Command Default

The next hop is not set to a tunnel interface.

Parameters

tunnel-id

Specifies the ID of the GRE tunnel interface. Valid values range from 1 to the maximum number of allowed Tunnel IDs configured in the system using the **system-max ip-tunnels** command.

Modes

Route map configuration mode

Usage Guidelines

Both IPv6 and IPv4 traffic can be redirected over a GRE tunnel using PBR.

This command sets the next hop to the GRE tunnel identified by the *tunnel-id* variable. Only GRE tunnels are supported by this command. The system will verify if a valid GRE tunnel with the specified *tunnel-id* variable exists. If the *tunnel-id* variable points to a tunnel other than a GRE tunnel or to a non-existent tunnel, the configuration is rejected.

The **no** form of the command removes the tunnel interface as the next hop.

Examples

The following example configures tunnel interface 1 as the next hop.

```
device(config)# interface tunnel 1
device(config-tnif-1)# tunnel source ethernet 1/1
device(config-tnif-1)# tunnel destination 10.2.2.1
device(config-tnif-1)# tunnel mode gre ip
device(config-tnif-1)# ipv6 address 2005:db8::1/64
device(config-tnif-1)# exit
device(config)# route-map Mall permit 1001
device(config-routemap Mall)# set next-hop-ip-tunnel 1
```

History

Release version	Command history
06.1.00	The support for the next hop type to redirect IPv6 traffic over GRE tunnel was extended to IPv6 PBR.

set next-hop-lsp

Configures an LSP as the next hop of a PBR route map.

Syntax

set next-hop-lsp *lsp-name*

no set next-hop-lsp *lsp-name*

Command Default

The next hop is not set to an LSP.

Parameters

lsp-name

Specifies the name of the configured LSP.

Modes

Route map configuration mode

Usage Guidelines

Both IPv6 and IPv4 traffic can be redirected over an MPLS tunnel using PBR. MPLS tunnel must be established before configuring next hop type as LSP.

The **no** form of the command removes the LSP as the next hop.

Examples

The following example configures LSP as the next hop.

```
device(config)# router mpls
device(config-mpls)# mpls-interface ethernet 6/1
device(config-mpls)# lsp t3
device(config-mpls-lsp-t3)# to 10.1.1.1
device(config-mpls-lsp-t3)# enable
device(config-mpls-lsp-t3)# exit
device(config)# route-map Mall permit 1001
device(config-routemap Mall)# set next-hop-lsp t3
```

History

Release version	Command history
06.1.00	The support for the next hop type LSP to redirect IPv6 traffic over MPLS tunnel was extended to IPv6 PBR.

set next-hop-tvf-domain

Configures a TVF domain as the next hop for a route map to support transparent VLAN flooding (TVF) with LAG load balancing.

Syntax

set next-hop-tvf-domain *tvf-domain-ID*

no set next-hop-tvf-domain *tvf-domain-ID*

Command Default

TVF domain as the route map next hop is not configured.

Parameters

tvf-domain-ID

Specifies the ID of the TVF domain. Valid values are from 1 through 2016.

Modes

Route map configuration mode

Usage Guidelines

The **no** form of the command removes the TVF domain as the route map next hop.

Examples

The following example configures a TVF domain 1 as the next hop for the test-route route map.

```
device(config)# route-map test-route permit 99
device(config-routemap test-route)# set next-hop-tvf-domain 1
```

History

Release version	Command history
6.0.00	This command was introduced.

sflow null0-sampling

Enables the null0 sampling.

Syntax

sflow null0-sampling *slot* **/***port*

no sflow null0-sampling *slot* **/***port*

Parameters

slot port

Enables null0 sampling for a specific slot and port.

Modes

Global configuration mode

History

Release	Command History
5.5.00	This command was modified to display sFlow null0 sampling status.

shortcuts isis

Forces ISIS IGP protocol not to use the configured LSP metric values for the shortcuts when doing SPF calculations.

Syntax

shortcuts isis { **level1** | **level2** } [**announce announce-metric** *value* | **ignore-lsp-metric**] [**announce** [**announce-metric** *value*]] [**relative-metric +/-** *value*]

no shortcuts isis { **level1** | **level2** } [**announce announce-metric** *value* | **ignore-lsp-metric**] [**announce** [**announce-metric** *value*]] [**relative-metric +/-** *value*]

Command Default

The configured LSP metric is used as the shortcut's cost when performing IGP SPF calculation.

Parameters

level1

A level1 router routes traffic only within the area that includes the router. To forward traffic to another area, a level1 router sends the traffic to the nearest level2 router.

level2

A level2 router routes traffic between areas within a domain.

announce

Announces tunnel into ISIS domain.

announce-metric *value*

Announces the metric value between 1-16777215. The default is 10.

ignore-lsp-metric

Ignore configured LSP metric as the shortcut's cost when performing IGP SPF calculation.

announce

Announce tunnel into ISIS domain.

announce-metric *value*

Announces the metric value between 1-16777215. The default is 10.

relative-metric

Configures relative metric.

+/- *value*

The + or – sign is required. + denotes a positive number. – denotes a negative number. For *value* , enter a value from 1 – 16777215. The default is 0 (zero).

Modes

MPLS LSP sub configuration mode (config-mpls-lsp-lsp*xxx*).

Usage Guidelines

Use the **no** form of this command without other optional keywords to disable this feature. The LSP must be disabled before configuring/de-configuring this feature.

When "ignore-lsp-metric" is enabled, ISIS will behave like the shortcut LSP metrics are not configured.

When announce is not enabled and a metric is not explicitly configured under the LSP configuration mode of the CLI, the relative metric is used to compute the shortcut cost.

Examples

The following example displays that when the tunnel is enabled, the user must disable it before enabling announce, then re-enable the tunnel.

```
device(config-mpls-lsp-tomu3)# disable
Disconnecting signaled LSP tomu3
device(config-mpls-lsp-tomu3)# shortcuts isis level2 announce
device(config-mpls-lsp-tomu3)# enable
Connecting signaled LSP tomu3
```

History

Release version	Command history
5.4.0	This command is modified to include the new option keyword **ignore-lsp-metric**. This is added to the existing shortcut command under the LSP configuration mode.

shortcuts ospf

Enables OSPF shortcuts over an LSP tunnel to forward traffic to destinations within an OSPF routing domain through an LSP tunnel.

Syntax

shortcuts ospf [**ignore-lsp-metric**]

no shortcuts ospf [**ignore-lsp-metric**]

Command Default

OSPF shortcuts over an LSP tunnel is not enabled.

Parameters

ignore-lsp-metric

Forces OSPF to ignore the configured LSP metric values as the shortcut cost when performing SFP calculations. The effective metric of the shortcut is derived by summing up all the path's cost spanned by the shortcut.

Modes

MPLS LSP mode.

Usage Guidelines

The LSPs must originate and terminate within the same OSPF area. When OSPF shortcuts over an LSP tunnel is enabled, OSPF directs routes that are reachable from the egress router of a shortcut-enabled LSP to an LSP tunnel as the outgoing interface.

The **no** form of this command without an option disables OSPF shortcuts over an LSP tunnel.

The **no** form of this command with the **ignore-lsp-metric** option disables the forcing of OSPF to ignore the configured LSP metric values as the shortcut cost when performing SFP calculations.

Examples

The following example is a configuration of the tunnel1 LSP to specify the egress router with a router ID of 10.2.2.2 and enable it for OSPF shortcuts.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# lsp tunnel1
device(config-mpls-lsp)# to 10.2.2.2
device(config-mpls-lsp)# shortcuts ospf
device(config-mpls-lsp)# enable
```

short-path-forwarding

Enables short-path forwarding on a Virtual Router Redundancy Protocol (VRRP) router.

Syntax

short-path-forwarding [**revert-priority** *number*]

no short-path-forwarding [**revert-priority** *number*]

Command Default

Short-path forwarding is disabled.

Parameters

revert-priority *number*

Allows additional control over short-path forwarding on a backup router. If you configure this option, the revert-priority number acts as a threshold for the current priority of the session, and only if the current priority is higher than the revert-priority will the backup router be able to route frames. The range of revert-priority is 1 to 254.

Modes

VRRP-E router configuration mode

Usage Guidelines

Short-path forwarding means that a backup physical router in a virtual router attempts to bypass the VRRP-E master router and directly forward packets through interfaces on the backup router.

This command can be used for VRRP-E, but not for VRRP. You can perform this configuration on a virtual Ethernet (VE) interface only.

Enter the **no short-path-forwarding** command to remove this configuration.

Examples

To enable short-path forwarding for a VRRP-E instance:

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# slow-start 40
device(config-vrrpe-router)# short-path-forwarding
```

Show Commands

show access-list accounting

Displays Access Control List (ACL) accounting statistics of IPv4 ACLs, IPv6 ACLs, and Layer 2 ACLs.

show access-list accounting brief [**rate-limit** | [**l2** | **uda**] [**policy-based-routing** [**omit-zero**]]]

show access-list accounting ethernet *slot/port* { **in** | **out** } [**rate-limit** | [**l2** | **uda**] [**policy-based-routing** [**omit-zero**]]]

show access-list accounting ve *ve-number* { **in** | **out** } [**rate-limit** | [**l2** | **uda**] [**policy-based-routing** [**omit-zero**]]]

brief
Displays the ACL accounting summary.

rate-limit
Displays rate-limit accounting information.

l2
Displays Layer 2 ACL accounting information.

uda
Displays UDA ACL accounting information.

policy-based-routing
Displays policy-based routing accounting information.

omit-zero
Specifies not to display ACL entry with 0 packet/bits.

in
Displays statistics of the inbound packets.

out
Displays statistics of the outbound packets.

ethernet *slot/port*
Displays the accounting statistics for ACLs on a physical interface.

ve *ve-number*
Displays the statistics for ACLs bound to ports that are members of a virtual routing interface.

User EXEC mode

The output displays information about IPv4 ACLs, IPv6 ACLs, or Layer 2 ACLs, based on the configuration of the port or interface. The clear command can be used clear the PBR statistics on the specified interface.

The **show access-list accounting** command displays the following information:

Output field	Description
Int	Identifies the interface.
In ACL	Displays the name of the ingress ACL.
Total In Hit	Displays the number of ingress-packet hits during the specified interval: • 1s—one second • 1m—one minute

Output field	Description
	• 5m—five minutes • acc—total accumulated packet hits
Out ACL	Displays the name of the egress ACL.
Total Out Hit	Displays the number of egress-packet hits during the specified interval.

The following example displays the incoming accounting information on a physical interface.

```
device(config)# enable-acl-counter
device# show access-list accounting ethernet 1/1 in
Inbound:
ACL 1
    0: permit host 29.7.51.11
       Hit count: (1 sec)                  0   (1 min)                  0
                  (5 min)                  0   (accum)                  0
    1: permit host 29.7.51.9
       Hit count: (1 sec)                  0   (1 min)                  0
                  (5 min)                  0   (accum)                  0
    2: permit host 29.7.51.10
       Hit count: (1 sec)                  0   (1 min)                  0
                  (5 min)                  0   (accum)                  0
    3: permit host 29.7.51.14
       Hit count: (1 sec)                  0   (1 min)                  0
                  (5 min)                  0   (accum)                  0
    4: permit host 29.7.51.15
       Hit count: (1 sec)                  0   (1 min)                  0
                  (5 min)                  0   (accum)                  0
```

The following example displays the Layer 2 PBR incoming accounting information on a physical interface.

```
device(config)# show access-list accounting ethernet 1/2 in l2 policy-based-routing
L2 Policy based Routing Accounting Information:

Routemap l2pbr10
ACL x10
    0:   10:  permit any any any etype any
       Hit count: (1 sec)                  0  (1 min)                   0
                  (5 min)                  0  (accum)                   0
```

The following example displays the general brief accounting summary.

```
device# show access-list accounting brief
    Int    In ACL              Total In Hit   Out ACL             Total Out Hit
    1/1         1                    0(1s)         2                    0(1s)
                                     0(1m)                              0(1m)
                                     0(5m)                              0(5m)
                                     0(ac)                              0(ac)
```

The following example displays the Layer 2 PBR accounting summary.

```
device# show access-list accounting brief l2 policy-based-routing
  1/1                           x10                    0(1s)
                                                       0(1m)
                                                       0(5m)
                                                       0(ac)

  4/2                           x10                    0(1s)
                                                       0(1m)
                                                       0(5m)
                                                       0(ac)
```

The following example displays the UDA PBR statistics on the specified interface.

```
device(config)# show access-list accounting ethernet 3/1 in uda policy-based-routing
Policy based Routing Accounting Information:
Routemap route1
ACL ACLNameTest112345679-023456789-0123456789
    0: sequence 10 permit 100 any any 1234 ffff any
        Hit count: (1 sec) 0 (1 min) 0
(5 min) 0 (accum) 0
                              0(ac)
```

Release version	Command history
5.8.00b	The **l2** option was introduced.
5.9.00	The command was modified to display the UDA PBR statistics on the specified interface.

show access-list bindings

Displays all access-lists bound to different interfaces. This includes both rule-based ACL and receive access-control list (rACL) information

Syntax

show access-list bindings

Modes

User EXEC node

Examples

The following example displays all access-list bindings.

```
Brocade(config)# show access-list bindings
L4 configuration:
!
interface ethe 2/1
 mac access-group SampleACL in
!
```

show access-list receive accounting

Displays accounting information for a receive access-control list (rACL) or brief information for all rACLs.

Syntax

show access-list receive accounting { *acl-num* | **name** *acl-name* | **brief** }

Parameters

acl-num

Specifies a receive ACL in number format. Valid values are 1 through 99 for standard ACLs and 100 through 199 for extended ACLs.

name *acl-name*

Specifies a receive ACL in name format.

brief

Displays receive-ACL accounting in brief.

Modes

User EXEC mode

Examples

The following example displays rACL accounting information for an ACL named "acl_ext1".

```
device(config)# show access-list receive accounting name acl_ext1
IP Receive ACL Accounting Information:
IP Receive ACL acl_ext1
ACL hit count for software processing (accum)                    0
HW counters:
    0: permit tcp any host 10.10.10.14
       Hit count: (1 sec)                  0   (1 min)          0
                  (5 min)                  0   (accum)          0
```

History

Release	Command History
5.6.00	This command was modified to support named ACLs, in addition to numbered ACLs.

show acl-policy

Displays the ACL policy configuration.

Syntax

show acl-policy

Modes

Privileged EXEC mode

Examples

The following example displays the ACL policy configuration.

```
device# show acl-policy
ACL-Policy configuration:
!
 display-config-format
 accounting-no-sort
 force-delete-bound-acl
 suppress-acl-seq
 display-def-acl-seq
 acl-skip-boot-checks
 acl-conflict-check
 acl-duplication-check
 display-pkt-bit-rate
 enable-acl-cam-sharing
 acl-frag-conservative
 enable-acl-counter
 statistics-load-interval  60
 suppress-ipv6-priority-mapping
 disable-acl-for-gre
 disable-acl-for-6to4
!
```

History

Release version	Command history
6.0.00	This command was introduced.

show arp

Displays an IP mechanism that the routers use to learn the Media Access Control (MAC) address of a device on the network.

Syntax

show arp [*ip-addr* [*ip-mask*] | *num-entries-to-skip* | **ethernet** *slot* **/** *port* | **mac-address** *xxxx.xxxx.xxxx* [*MAC-mask*] | **vrf** *vrf-name*]

Parameters

ip_addr

Specifies IP address.

ip_mask

Specifies IP subnet.

num-entries-to-skip

Number of entries to skip.

ethernet *slot/port*

Displays specified ethernet port.

mac-address *xxxx.xxxx.xxxx*

Displays the mac address of the specified entry.

MAC-mask

Specifies a mask for display of multiple MAC addresses.

vrf *vrf_name*

Displays ARP entries belonging to a given VRF instance.

Modes

User EXEC mode

Usage Guidelines

show arp

This command operates in all modes.

Command Output

The **show arp** command displays the following information:

Output field	Description
IP Address	The IP address of the entry.
MAC Address	The MAC address of the entry.

Output field	Description
Type	Displays the type of entry. The options are: • Static: The Layer 3 switch loaded the entry from the static ARP table when the device for the entry was connected to the Layer 3 switch. • Dynamic: The Layer 3 switch learned the entry from an incoming packet. • DHCP - The Layer 3 Switch learned the entry from the DHCP binding address table. In this case, the port number is not available until the entry gets resolved through ARP.
Age	The number of minutes before which the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.
Port/Port	The 'To' and 'From' ports. If the ARP entry type is DHCP, the port number is not available until the entry gets resolved through ARP.
Vpls-Id:Vlan	Displays VPLS identification information.
Vpls-Id:Peer	Displays VPLS peer information.

Examples

The following example displays the **show arp** command output:

```
device(config)# show arp
Total number of ARP entries: 4
Entries in default routing instance:
IP Address    MAC Address     Type    Age   Port/Port (Vpls-Id:Vlan)/(Vpls-Id:Peer)
10.25.104.1   0000.0012.3eb5  Static  None  4/1       (101, 26)
10.25.104.3   0000.000f.c200  Dynamc  0     mgmt1
10.1.1.2      0000.00f8.0090  Dynamc  1     mgmt1
10.25.104.1   0000.0012.3eb5  Static  None            (21,10.32.332.1)
```

show arp-guard-access-list

Displays details for a specified ARP-guard access list (ACL) or all ARP-guard ACLs.

Syntax

show arp-guard-access-list { **all** | **name** *arp-guard-access-list* }

Parameters

all

Specifies all ARP-guard ACLs.

name *arp-guard-access-list*

Specifies the name of an ARP-guard access list.

Modes

User EXEC mode

Examples

The following example displays information about the ARP guard access list named C5-global-arp.

```
device# show arp-guard-access-list name C5-global-arp
Arp-Guard : C5-global-arp
Number of rules : 6
Number of Ports : 16
Rules configured
 permit  40 31.0.8.1 0012.f290.7400
 permit  1500 31.0.10.2 0000.0015.0000
 permit  1001 100.0.0.2 0024.38a3.6e00
 permit  20 41.0.100.1 0024.38a3.6e00
 permit  80 51.0.4.2 748e.f874.4900
 permit  any 31.0.11.1 0012.f290.7400
```

The following example displays information about all the ARP guard access list.

```
device# show arp-guard-access-list all
Arp-guard configuration:
!
arp-guard-access-list C5-8
!
arp-guard-access-list MCT-A3
 permit  any 31.0.10.2 0000.0300.0000
 permit  any 31.0.10.3 0000.0300.0001
 permit  any 31.0.10.4 0000.0300.0002
 permit  any 31.0.10.5 0000.0300.0003
 permit  any 31.0.11.1 any
 permit  any 31.0.11.2 any
 permit  any 31.0.11.3 any
!
arp-guard-access-list C5-global-arp
 permit  40 31.0.8.1 0012.f290.7400
 permit  1500 31.0.10.2 0000.0015.0000
 permit  1001 100.0.0.2 0024.38a3.6e00
 permit  20 41.0.100.1 0024.38a3.6e00
 permit  80 51.0.4.2 748e.f874.4900
 permit  any 31.0.11.1 0012.f290.7400
!
arp-guard-access-list AS201
 permit  any 1.1.1.1 any
 permit  any 1.1.1.1 0001.0001.0001
!
```

History

Release version	Command history
R05.7.00	This command was introduced.

show arp-guard port-bindings

Displays list of ports associated with an ARP-guard access-list (ACL) or with all ARP-guard ACLs.

Syntax

show arp-guard port-bindings { *arp-guard-access-list* | **all** }

Parameters

arp-guard-access-list

Displays port-binding associations for an ARP-guard access list.

all

Displays port-binding associations for all ARP-guard ACLs.

Modes

User EXEC mode

Usage Guidelines

This command can be entered in most configuration modes. See the Examples section for several examples in different configuration modes.

Command Output

The **show arp-guard port-bindings** command displays the following information:

Output field	Description
Arp-Guard	Displays the name of the ARP-guard.
Number of Ports	Displays the total number of ports associated with this ARP-guard.
Port Lists	Displays the list of ports associated with that ARP-guard.

Examples

The following example displays information about the ARP-guard port bindings for AS200.

```
device(config-if-e10000-1/8)# show arp-guard port-bindings AS200
Arp-Guard : AS200
Number of Ports : 1
Port Lists : ethe 1/8
```

The following example displays information about the ports associated with ARP-guard.

```
device# show arp-guard port-bindings all
Arp-Guard Port Bindings:

Arp-Guard        : ag1
 Number of Ports  : 0

Arp-Guard        : ag2
 Number of Ports  : 2
  Ethe 1/2        Log : Disabled
  Ethe 1/4        Log : Disabled

Arp-Guard        : ag3
 Number of Ports  : 8
  Ethe 1/1        Log : Disabled
  Ethe 2/1        Log : Enabled       Num of violations : Default
  Ethe 2/2        Log : Enabled       Num of violations : 32
  Ethe 2/3        Log : Enabled       Num of violations : 32
  Ethe 2/4        Log : Enabled       Num of violations : 32
  Ethe 2/6        Log : Disabled
  Ethe 3/1        Log : Enabled       Num of violations : Default
  Ethe 4/1        Log : Enabled       Num of violations : Default
```

History

Release version	Command history
5.7.00	This command was introduced.

show arp-guard statistics ethernet

Displays ARP-guard statistical information.

Syntax

show arp-guard statistics ethernet { **all** | *slot/port* [**vlan** *vlan-id*] }

Parameters

all

Displays all ARP-guard port statistics.

slot/port

Displays statistics specific to a port.

vlan *vlan-id*

Displays statistics specific to a VLAN on a port. The VLAN ID range is from 1 through 4090.

Modes

User EXEC mode

Usage Guidelines

This command displays statistics for LAG primary ports, but not for secondary ports.

Command Output

The **show arp-guard statistics ethernet** command displays the following information:

Output field	Description
Port	The port number.
Vlan-id	The VLAN ID.
Total_Arp_pkts_captured	The total number of ARP packets captured.
Total_Arp_pkts_forwarded	The total number of ARP packets forwarded
Total_Arp_pkts_dropped	The total number of ARP packets dropped
LAG : Prim	Displayed only in the show arp-guard statistics ethernet all alone. To denote LAG ID and its Primary port for that LAG associated with all the ARP-guard enabled ports.

Examples

The following example displays statistics information for all the ports.

```
device(config)# show arp-guard statistics ethernet all
Port         Vlan-id  Total_Arp_pkts_captured  Total_Arp_pkts_forwarded  Total_Arp_pkts_dropped  LAG :
Prim
1/1 (Def/Untag)1            0                        0                       0
1/1            3            10000                    9000                    100
1/1            2            10000                    9000                    100
2/1 (Def/Untag)1            0                        0                       0
2/1            2            10000                    9000                    100
2/1            4            10000                    9000                    100
2/1            5            10000                    9000                    100
```

The following example displays statistics information for any individual port.

```
device(config)# show arp-guard statistics ethernet 1/1
Port         Vlan-id  Total_Arp_pkts_captured  Total_Arp_pkts_forwarded  Total_Arp_pkts_dropped  LAG :
Prim
1/1 (Def/Untag)1            0                      0                       0
1/1            3            10000                  9000                    100
1/1            2            10000                  9000                    100
```

The following example displays statistics information for a VLAN of the ARP-guard-enabled port

```
device# show arp-guard statistics ethernet 1/1 vlan 2
Port           Vlan-id    Total_Arp_pkts_captured  Total_Arp_pkts_forwarded  Total_Arp_pkts_dropped
1/1                     2            10000
9000                                  100
```

History

Release version	Command history
R05.7.00	This command was introduced.

show bfd

Displays Bidirectional Forwarding Detection (BFD) information.

Syntax

show bfd

Modes

User 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.
Use PBIF Assist	Specifies the status of PCI Bus Interface (PBIF) Assist.
Current Registered Protocols	Specifies which protocols are registered to use BFD on the device. Possible values are mpls/0, ospf/0, ospf6/0, or isis_task/0.
All Sessions	
Current:	The number of BFD sessions currently operating on the device.
Maximum Allowed	The maximum number of BFD sessions that are allowed on the device. The maximum number of sessions supported is 250 for Brocade NetIron MLX Series devices and Brocade NetIron XMR Series devices and 40 for Brocade NetIron CES Series devices.
Maximum 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.
LP Sessions:	
Maximum Allowed on LP	The maximum number of BFD sessions that are allowed on an interface module. The maximum number of sessions supported on an interface module is 40 for Brocade NetIron XMR Series devices and Brocade NetIron MLX Series devices, and 20 for Brocade NetIron CES Series devices.
Maximum Exceeded Count for LPs	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 an interface module.
LP	The number of the interface module for which the Current Session Count is displayed.
TX/RX Sessions	The number of Transmit (Tx) and Receive (Rx) BFD sessions currently operating on the specified interface module.
BFD Enabled ports count	The number of ports on the device that have been enabled for BFD.
Port	The port that BFD is enabled on.
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 non-operational.
Sessions	The number of BFD sessions originating on this port.

Examples

The following example displays BFD information for the device.

```
device# show bfd

BFD State: ENABLED Version: 1 Use PBIF Assist: Y
Current Registered Protocols: ospf/0  ospf6/0
All Sessions: Current: 4 Maximum Allowed: 100 Maximum Exceeded Count: 0
LP Sessions: Maximum Allowed on LP: 40  Maximum Exceeded Count for LPs: 0
LP Tx/Rx Sessions LP Tx/Rx Sessions LP Tx/Rx Sessions LP Tx/Rx Sessions
1   4/4           2   2/2           3  0/0           4  0/0
5   0/0           6   0/0           7  0/0           8  0/0
9   0/0           10  0/0           11 0/0           12 0/0
13  0/0           14  0/0           15 0/0           16 0/0
BFD Enabled ports count: 2
Port       MinTx       MinRx       Mult Sessions
eth 2/1    100         100         3    2
eth 3/1    100         100         3    2
```

History

Release version	Command history
5.6.00	This command was modified to include MPLS in the registered protocol list. In addition, the number of sessions on the LP is shown separately as TX and RX.

show bfd applications

Displays Bidirectional Forwarding Detection (BFD) registered protocol information.

Syntax

show bfd applications

Modes

User EXEC mode

Command Output

The **show bfd applications** command displays the following information:

Output field	Description
Registered Protocols Count	Total number of protocols registered to use BFD on the device.
Protocol	Which protocols are registered to use BFD on the device.
VRFID	The VRFID of the protocol.
Parameter	The parameter value passed by the protocol during registration with BFD.
HoldoverInterval	The time by which the BFD session down notification is delayed. If within that holdover time, the BFD session is up, then it is not notified of the BFD session flap.

Examples

The following example displays BFD registered protocol information for the device.

```
device# show bfd applications

Registered Protocols Count: 3
Protocol  VRFID     Parameter HoldoverInterval
isis      0         0         2
ospf6     0         1         10
ospf      0         0         5
```

History

Release version	Command history
5.6.00	The command was modified to include MPLS information.

show bfd mpls

Displays information about MPLS Bi-Directional Forwarding (BFD) sessions. You can filter BFD sessions based on LSP name or egress RSVP session ID.

Syntax

show bfd mpls

show bfd mpls detail

show bfd mpls lsp *lsp-name*

show bfd mpls rsvp-session *src_addr dest-addr tunnel-id*

Parameters

detail

Displays the MPLS BFD session in detail.

lsp *lsp-name*

Displays the MPLS BFD session associated with a specific LSP.

rsvp-session *src_addr dest-addr tunnel-id*

Displays the MPLS BFD session associated with the egress RSVP session specified using the source address, destination address, and tunnel ID options.

Modes

User EXEC mode

Usage Guidelines

If no optional keywords are entered, information about all MPLS BFD sessions is displayed. You can filter BFD session based on LSP name or egress RSVP session ID or show detailed MPLS BFD information. For MPLS BFD sessions associated with LSP, the LSP name is displayed. For a BFD session associated with an egress RSVP session, the RSVP session ID issued to identify the BFD session is displayed.

History

Release	Command history
5.6.00	This command was introduced.

show bfd neighbors

Displays detailed Bidirectional Forwarding Detection (BFD) neighbor information.

Syntax

show bfd neighbors [*ip-address* | *ipv6-address*]

Parameters

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Command Output

The **show bfd neighbors** command displays the following information:

Output field	Description
Total number of Neighbor entries	The number of neighbors that have established BFD sessions with ports on this device.
NeighborAddress	The IPv4 or IPv6 address of the remote peer.
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.
Interface	The logical port (physical or virtual port) on which the peer is known.
Holddown	The interval in milliseconds after which the session will transition to the down state if no message is received.
Interval	The interval in milliseconds at which the local device sends BFD messages to the remote peer.
R/H	R - Heard from Remote. Displays Y for Yes or N for No. H - Hops. Display S for single hop or M for multihop.

Examples

The following example displays BFD neighbor information for the device.

```
device# show bfd neighbors
Total number of Neighbor entries: 2
NeighborAddress          State   Interface Holddown  Interval  R/H
10.14.1.1                UP      eth 3/1   300000    100000    Y/S
10.2.1.1                 UP      eth 2/1   300000    100000    Y/S
```

show bfd neighbors bgp

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for BGP.

Syntax

show bfd neighbors bgp [**details**] [*ip-address* | *ipv6-address*]

Parameters

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Command Output

The **show bfd neighbors bgp details** command displays the following information:

Output field	Description
Total Entries	Total number of BFD sessions.
NeighborAddress	IPv4 or IPv6 address of the remote peer.
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.
Interface	The logical port on which the peer is known.
Holddown	The interval in milliseconds after which the session will transition to the down state if no message is received.
Interval	The interval in milliseconds at which the local device sends BFD messages to the remote peer.
R/H	R - Heard from Remote. Displays Y for Yes or N for No. H - Hops. Display S for single hop or M for multihop.
Registered Protocols	Specifies which protocols are registered to use BFD on this port.
Local:	The local device
Disc	Value of the local discriminator field in the BFD control message as used by the local device in the last message sent.

Output field	Description
Diag	Value of the diagnostic field in the BFD control message as used by the local device in the last message sent.
Demand	Value of the demand bit in the BFD control message as used by the local device in the last message sent.
Poll	Value of the poll bit in the BFD control message as used by the local device in the last message sent.
MinTxInterval	The interval in milliseconds during which the device will send a BFD message from this local neighbor port to the peer.
MinRxInterval	The interval in milliseconds that the neighbor device waits to receive a BFD message from the peer on this local port.
Multiplier	The number of times the neighbor device will wait for the MinRxInterval time on this port before it determines the peer device is non-operational.
Remote:	Remote peer.
Disc	Value of the local discriminator field in the BFD control message as received in the last message sent by the remote peer.
Diag	Value of the diagnostic field in the BFD control message as received in the last message sent by the remote peer.
Demand	Value of the demand bit in the BFD control message as received in the last message sent by the remote peer.
Poll	Value of the poll bit in the BFD control message as received in the last message sent by the remote peer.
MinTxInterval	The interval in milliseconds during which the device will send a BFD message from the remote neighbor port to the peer.
MinRxInterval	The interval in milliseconds that the neighbor device waits to receive a BFD message from the 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 the peer device is non-operational.
Stats:	Statistics
Rx	Total number of BFD control messages received from the remote peer.
Tx	Total number of BFD control messages sent to the remote peer.
SessionUpCount	The number of times the session has transitioned to the up state.
SysUpTime	The amount of time that the system has been up.
Session Uptime	The amount of time the session has been in the up state.
LastSessionDownTimestamp	The system time at which the session last transitioned from the up state to some other state.
Physical Port	The physical port on which the peer is known.
Vlan Id	The VLAN ID of the VLAN on which the physical port is resident.

Examples

The following example displays BFD neighbor information for BGP for the device.

```
device# show bfd neighbors bgp

Neighbor AS4 Capability Negotiation:
As-path attribute count: 2
Outbound Policy Group:
ID: 1, Use Count: 3
BFD:Enabled,BFDSessionState:UP,Multihop:Yes
LastBGP-BFDEvent:RX:Up,BGP-BFDError:No Error
NegotiatedTime(msec):Tx:1000000,Rx:1000000,BFDHoldTime:3000000
HoldOverTime(sec) Configured:22,Current:0,DownCount:0
TCP Connection state: ESTABLISHED, flags:00000044 (0,0)
Maximum segment size: 1460
```

The following example displays detailed BFD neighbor information for BGP for a Brocade NetIron MLX Series or Brocade NetIron XMR Series device.

```
device# show bfd neighbors bgp details

Total Entries:4 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress               State  Interface Holddown   Interval R/H
10.101.101.100                UP     ve 3      3000000    1000000  Y/M
  Registered Protocols(Protocol/VRFID): bgp/0
  Local: Disc: 26, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Remote: Disc: 7, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Stats: RX: 14682 TX: 12364 SessionUpCount: 1 at SysUpTime: 0:2:46:24.725
  Session Uptime: 0:1:37:50.600, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3
NeighborAddress                        State  Interface Holddown   Interval R/H
10.100.100.100                         UP     ve 3      3000000    1000000  Y/M
  Registered Protocols(Protocol/VRFID): bgp/0
  Local: Disc: 27, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Remote: Disc: 8, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Stats: RX: 14232 TX: 12046 SessionUpCount: 1 at SysUpTime: 0:2:46:24.725
  Session Uptime: 0:1:37:49.650, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3
NeighborAddress                         State  Interface Holddown   Interval R/H
10.1.1.1                                 UP     ve 3      3000000    1000000  Y/M
  Registered Protocols(Protocol/VRFID): bgp/0
  Local: Disc: 28, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Remote: Disc: 9, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Stats: RX: 15652 TX: 12044 SessionUpCount: 1 at SysUpTime: 0:2:46:24.725
  Session Uptime: 0:1:37:48.725, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3
NeighborAddress                        State  Interface Holddown   Interval R/H
10.102.102.100                         UP     ve 3      3000000    1000000  Y/M
  Registered Protocols(Protocol/VRFID): bgp/0
  Local: Disc: 29, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Remote: Disc: 10, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
  Stats: RX: 14232 TX: 12044 SessionUpCount: 1 at SysUpTime: 0:2:46:24.725
  Session Uptime: 0:1:37:48.550, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3
```

The following example displays detailed BFD neighbor information for BGP for a Brocade NetIron CES Series or Brocade NetIron CER Series device.

```
device# show bfd neighbors bgp details

Total Entries:1 R:RXRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress                State  Interface Holddown   Interval R/H
fe80::224:38ff:fe79:9310       UP     eth 1/17  1500000    500000   Y/S
  Registered Protocols(Protocol/VRFID): bgp/0
  Local: Disc: 8, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 500000, MinRxInterval: 500000, Multiplier: 3
Remote: Disc: 2, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 500000, MinRxInterval: 500000, Multiplier: 3
Stats: RX: 160394 TX: 142648 SessionUpCount: 1 at SysUpTime: 5:17:14:13.225
  Session Uptime: 0:17:49:42.100, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/17,RX: eth 1/17,Vlan Id: 1
  Using PBIF Assist: Y
```

show bfd neighbors details

Displays detailed Bidirectional Forwarding Detection (BFD) neighbor information.

Syntax

show bfd neighbors details [*ip-address* | *ipv6-address*]

Parameters

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Command Output

The **show bfd neighbors details** command displays the following information:

Output field	Description
Total number of Neighbor entries	Total number of BFD sessions.
NeighborAddress	IPv4 or IPv6 address of the remote peer.
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.
Interface	The logical port on which the peer is known.
Holddown	The interval in milliseconds after which the session will transition to the down state if no message is received.
Interval	The interval in milliseconds at which the local device sends BFD messages to the remote peer.
R/H	R - Heard from Remote. Displays Y for Yes or N for No. H - Hops. Display S for single hop or M for multihop.
Registered Protocols	Specifies which protocols are registered to use BFD on this port.
Local:	The local device
Disc	Value of the local discriminator field in the BFD control message as used by the local device in the last message sent.
Diag	Value of the diagnostic field in the BFD control message as used by the local device in the last message sent.
Demand	Value of the demand bit in the BFD control message as used by the local device in the last message sent.

Output field	Description
Poll	Value of the poll bit in the BFD control message as used by the local device in the last message sent.
MinTxInterval	The interval in milliseconds between which the device will send a BFD message from this local neighbor port to its peer.
MinRxInterval	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 non-operational.
Remote:	Remote peer.
Disc	Value of the local discriminator field in the BFD control message as received in the last message sent by the remote peer.
Diag	Value of the diagnostic field in the BFD control message as received in the last message sent by the remote peer.
Demand	Value of the demand bit in the BFD control message as received in the last message sent by the remote peer.
Poll	Value of the poll bit in the BFD control message as received in the last message sent by the remote peer.
MinTxInterval	The interval in milliseconds between which the device will send a BFD message from the remote neighbor port to its peer.
MinRxInterval	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 non-operational.
Stats	Statistics
Rx	Total number of BFD control messages received from the remote peer.
Tx	Total number of BFD control messages sent to the remote peer.
SessionUpCount	The number of times the session has transitioned to the up state.
SysUpTime	The amount of time that the system has been up.
Session Uptime	The amount of time the session has been in the up state.
LastSessionDownTimestamp	The system time at which the session last transitioned from the up state to some other state.
Physical Port	The physical port on which the peer is known.
Vlan Id	The VLAN ID of the VLAN on which the physical port is resident
Session	Session details
Using PBIF Assist	Y for Yes: PBIF Assist is used for this BFD session. N for No: PBIF is not used for this BFD session.

Examples

The following example displays detailed BFD neighbor information for the device.

```
device# show bfd neighbors details
Total number of Neighbor entries: 1
NeighborAddress                         State   Interface Holddown  Interval  R/H
10.14.1.1                               UP      ve 50     300000    100000    Y/S
  Registered Protocols(Protocol/VRFID): ospf/0
  Local: Disc: 1, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Remote: Disc: 22, Diag: 7, Demand: 0 Poll: 0
          MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Stats: RX: 72089 TX: 72101 SessionUpCount: 1 at SysUpTime: 0:1:30:54.775
  Session Uptime: 0:1:30:6.375, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port: eth 4/1, Vlan Id: 50,Session: Active
Using PBIF Assist: Y
```

show bfd neighbors interface

Displays Bidirectional Forwarding Detection (BFD) neighbor information about specified interfaces.

Syntax

show bfd neighbors interface [**ethernet** *slot/port* | **pos** *slot/port* | **ve** *vlan_id*] [**details**] [*ip-address* | *ipv6-address*]

Parameters

ethernet *slot /port*

Specifies an Ethernet interface with a valid slot and port number.

pos *slot /port*

Specifies an Packet over SONET (POS) interface with a valid slot and port number.

ve *vlan-id*

Specifies a virtual Ethernet (VE) interface.

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for the Ethernet 1/1 interface.

```
device# show bfd neighbors interface ethernet 1/1

 BFD State: ENABLED Version: 1 Use PBIF Assist: Y SH setup delay 180 MH setup delay 0
 Current Registered Protocols: mpls/0  ospf/2  ospf6/0  ospf/4  ospf/0
 All Sessions: Current: 0 Maximum Allowed: 250 Maximum Exceeded Count: 0
 Maximum TX/RX Sessions Allowed on LP: 80  Maximum Session Exceeded Count for LPs: 0
   LP Tx/Rx Sessions LP Tx/Rx Sessions LP Tx/Rx Sessions LP Tx/Rx Sessions
   1   0/0           2   0/0           3   0/0           4   0/0
 BFD Enabled ports count: 1
 Port       MinTx       MinRx       Mult Sessions
 eth 1/1    55          55          5    0
```

show bfd neighbors isis

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for IS-IS.

Syntax

show bfd neighbors isis [**details**] [*ip-address* | *ipv6-address*]

Parameters

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for IS-IS.

```
device# show bfd neighbors isis

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress       State  Interface       Holddown   Interval  R/H
10.40.40.10           UP     eth 3/6         900000     300000    Y/S
```

The following example displays detailed BFD neighbor information for IS-IS.

```
device# show bfd neighbors isis details

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress          State  Interface       Holddown   Interval  R/H
10.40.40.10              UP     eth 3/6         900000     300000    Y/S
  Registered Protocols(Protocol/VRFID): isis/0
  Local: Disc: 9, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 300000, MinRxInterval: 300000, Multiplier: 3
  Remote: Disc: 5, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 300000, MinRxInterval: 300000, Multiplier: 3
  Stats: RX: 226 TX: 252 SessionUpCount: 1 at SysUpTime: 2:0:25:44.306
  Session Uptime: 0:0:0:59.278, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 3/6,RX: eth 3/6,Vlan Id: 1
  Using PBIF Assist: Y
```

show bfd neighbors ospf

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for OSPFv2.

Syntax

show bfd neighbors ospf [**details**] [*ip-address* | *ipv6-address*]

Parameters

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for OSPFv2.

```
device# show bfd neighbors ospf

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress               State  Interface       Holddown   Interval  R/H
1.1.1.1                       UP     eth 1/2         300000     100000    Y/S
```

The following example displays detailed BFD neighbor information for OSPFv2.

```
device# show bfd neighbors ospf details

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress               State  Interface       Holddown   Interval  R/H
1.1.1.2                       UP     eth 1/2         300000     100000    Y/S
  Registered Protocols(Protocol/VRFID): static/0 ospf/0
  Local: Disc: 1, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Remote: Disc: 1, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Stats: RX: 1053134 TX: 917679 SessionUpCount: 1 at SysUpTime: 0:23:30:4.55
  Session Uptime: 0:23:24:40.367, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/2,RX: eth 1/2,Vlan Id: 1
  Using PBIF Assist: Y
```

show bfd neighbors ospf6

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for OSPFv3.

Syntax

show bfd neighbors ospf6 [**details**] [*ip-address* | *ipv6-address*]

Parameters

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for OSPFv3.

```
device# show bfd neighbors ospf6

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress                         State  Interface       Holddown    Interval  R/H
fe80::21b:edff:fe3b:8601                UP     eth 1/2         300000      100000    Y/S
```

The following example displays detailed BFD neighbor information for OSPFv3.

```
device# show bfd neighbors ospf6 details

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress                State  Interface       Holddown    Interval  R/H
fe80::21b:edff:fe3b:8601       UP     eth 1/2         300000      100000    Y/S
  Registered Protocols(Protocol/VRFID): ospf6/0
  Local: Disc: 2, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Remote: Disc: 2, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Stats: RX: 1046743 TX: 912150 SessionUpCount: 1 at SysUpTime: 0:23:30:25.808
  Session Uptime: 0:23:16:8.793, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/2,RX: eth 1/2,Vlan Id: 1
  Using PBIF Assist: Y
```

show bfd neighbors static

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for IP static routes.

Syntax

show bfd neighbors static [**details**] [*ip-address* | *ipv6-address*]

Parameters

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for IP static routes.

```
device# show bfd neighbors static

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress               State  Interface       Holddown   Interval  R/H
1.1.1.1                       UP     eth 1/2         300000     100000    Y/S
```

The following example displays detailed BFD neighbor information for IP static routes.

```
device# show bfd neighbors static details

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress               State  Interface       Holddown   Interval  R/H
1.1.1.2                       UP     eth 1/2         300000     100000    Y/S
  Registered Protocols(Protocol/VRFID): static/0 ospf/0
  Local: Disc: 1, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Remote: Disc: 1, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Stats: RX: 1054000 TX: 918434 SessionUpCount: 1 at SysUpTime: 0:23:31:13.409
  Session Uptime: 0:23:25:49.719, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/2,RX: eth 1/2,Vlan Id: 1
  Using PBIF Assist: Y
```

show bfd neighbors static6

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for IPv6 static routes.

Syntax

show bfd neighbors static6 [**details**] [*ip-address* | *ipv6-address*]

Parameters

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for IPv6 static routes.

```
device# show bfd neighbors static6

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress               State  Interface       Holddown   Interval  R/H
1::1                          UP     eth 1/2         300000     100000    Y/S
```

The following example displays detailed BFD neighbor information for IPv6 static routes.

```
device# show bfd neighbors static6 details

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress               State  Interface       Holddown   Interval  R/H
1::1                          UP     eth 1/2         300000     100000    Y/S
  Registered Protocols(Protocol/VRFID): static6/0
  Local: Disc: 3, Diag: 0, Demand: 0 Poll: 0
         MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Remote: Disc: 3, Diag: 0, Demand: 0 Poll: 0
          MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Stats: RX: 1192696 TX: 1023053 SessionUpCount: 1 at SysUpTime: 0:23:31:37.757
  Session Uptime: 0:23:11:58.266, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/2,RX: eth 1/2,Vlan Id: 1
  Using PBIF Assist: Y
```

show bip slot

Displays a table that contains the lane number for a Physical Coding Sublayer (PCS) lane and a count of Bit Interleaved Parity (BIP) errors for that PCS lane, for each lane where a counter is active.

Syntax

show bip slot *slot_number*

Parameters

slot_number

Specifies the slot number for which the BIP information is to be displayed.

Modes

User EXEC mode.

Usage Guidelines

Command Output

The **show bip slot** command displays the following information:

Output field	Description
Lane	The PCS lane on the port.
Count	The value of the counter associated with the lane.

Examples

The following example shows the **show bip slot** command:

```
device# show bip slot 3
Port 3/1:
PCS Lane BIP Error Counters :
*****************************
    Lane00  : 001           Lane01  : 001
    Lane02  : 001           Lane03  : 001
    Lane04  : 001           Lane05  : 001
    Lane06  : 001           Lane07  : 001
    Lane08  : 001           Lane09  : 001
    Lane10  : 001           Lane11  : 001
    Lane12  : 001           Lane13  : 001
    Lane14  : 001           Lane15  : 001
    Lane16  : 001           Lane17  : 001
    Lane18  : 001           Lane19  : 001
Port 3/2:
PCS Lane BIP Error Counters :
*****************************
    Lane00  : 000           Lane01  : 000
    Lane02  : 000           Lane03  : 000
    Lane04  : 000           Lane05  : 000
    Lane06  : 000           Lane07  : 000
    Lane08  : 000           Lane09  : 000
    Lane10  : 000           Lane11  : 000
    Lane12  : 000           Lane13  : 000
    Lane14  : 000           Lane15  : 000
    Lane16  : 000           Lane17  : 000
    Lane18  : 000           Lane19  : 000
All show BIP done
```

History

Release	Command History
05.8.00a	This command was modified

show cam-detail-eth

Displays Content Addressable Memory (CAM) programming information for a specific Layer 2 CAM flow entry.

Syntax

show cam-detail-eth *slot/port mac_address* [**vlan** *vlan_id* | **vpls-vlan** *vlan_id*]

Parameters

slot/port
: Specifies the LP module slot and port number.

mac_address
: Specifies the MAC address of the Layer 2 PRAM entry.

vlan*vlan_id*
: Specifies the VLAN ID number.

vpls-vlan*vlan_id*
: Specifies the VPLS-VLAN ID number

Modes

Privileged EXEC level.

Usage Guidelines

Use this command to retrieve and display Layer 2 CAM or PRAM flow entry information without using a separate sequence of debugging commands. The command eliminates the need to remember indices information required to capture Layer 2 flow information by doing all the work in the back-end. The command only uses the MAC address or the VLAN ID or VPLS VLAN ID for Layer 2 to read and display information for a specific Layer 2 PRAM entry.

The command is supported only on the LP module.

NOTE
The command is supported on Brocade NetIron XMR Series and Brocade MLX Series devices.

Examples

The **show cam-detail-eth** command displays the following information on 2/8 with address fdab:1234:4567 of VLAN 100:

```
device# show cam-detail-eth 2/8 fdab:1234:4567 vlan 100
**********************(show cam ethernet <slot/port>) output*****************************************
LP Index MAC            Age Port  IFL/ Out IF PRAM  Type
    (Hex)                         VLAN        (Hex)
2  4ffff ffff.ffff.0000 Dis 2/8   100    CPU    3ff5b DA
**********************(dm cam [<interface> <index>]) output*****************************************
(CAM 0x0004ffff): ffff.ffff.0000/ffff.ffff.0000 VPN 0/0
**********************(dm cam2pram <interface> <index>) output***********************************
(CAM2PRAM entry 0x09fffe): 0003ff5b cam_idx: 0x0004ffff
(CAM2PRAM entry 0x09ffff [MAC SA or Right IP]): 0003ff80
**********************(dm pram <interface> <index> mac-da) output*********************************
PRAM 0x3ff5b 255[00000000:00000000:00000000:00000000]128
             127[00000000:00100000:8600800f:05f00000]0
********************PRAM MAC entry (DA)**********************
ALT SRC PORT    1          Use alternate src port
MONITOR         0          Copy packet to MONITOR port
CPU             0          Packet must be copied to CPU
DISCARD INVLD   0          Discard if lookup invalid
DISCARD PACKET  0          Force packet to be discarded
USE FID         1          Use FID from this PRAM entry
USE QOS ID      1          Use QOS ID for rate limiting
INNER VLAN VALID   0000      Inner Vlan Valid
QOS ID          0x20       QOS rate limiting ID
VALID           0x000000f     Per-port entry valid
FID             0x05f0     Forwarding ID
TRUNK ADJUST    0          Adjust FID based on trunk index
DIS_QOS_OVERRIDE 0         Disable QOS Override
PRIORITY_FORCE  0          Force pram priority to packet
PRIORITY        0          Packet priority
FASTPATH ENA    0          DA/SA is a known router
IGNORE BLOCK    0          Ignore port or RX block
DPA KNOWN       0          DPA associated with this DA is known
US              0          Set RX_US bit
LOCAL ADDRESS   0          Address was learned locally
IGNORE US       0          Ignore router MAC
IGNORE ACLRES   0          Ignore ACL lookup
INNER VLAN      0000        Replacement Inner Vlan ID
PRAM TYPE       1          PRAM Entry Type
TRUNK ID        0           Trunk group ID
REPLACE VLAN    0          Use Outer Replacement VLAN ID
OUTER VLAN      0         Outer Replacement VLAN ID
MUTLICAST VLAN  0          Set Multicast VLAN Flag
MATCH ALL DA    0          Match All DA Entry
LOCAL_SWITCHING (MAC-DA only) 0          Perform L2 DA forwarding
DONT MODIFY PKT 0          Send Unmodified Copy
SOURCE PORT     0x00      Source Port of CAM entry
HPORT VALID     0x00      Host port per port entry valid
BOGUS  LABEL BIT    0      Indicates if this label is used for single hop acct
TAG               0      VPLS Tag Mode support
NEXT HOP INDEX    0      next hop router index
PRAM MCAST SKIP MCAST    0         MCT/PBB mask indicating where to forward
PRAM EGRESS ID HI  0      higher 12-bits of PRAM_EGRESS_ID for HQOS support
PRAM EGRESS ID LO  0      Lower 4-bits of PRAM_EGRESS_ID for HQOS support
PUSH OUTER LABEL 0       Push the Outer Label
INNER LABEL 0   inner label
OUTER LABEL 0   outer label
REPLACE INNER VLAN  0          Use replacement inner VLAN
**********************(dm fid-entry-table <fid>)
output*************************************************
FID 25 (00000019): cpu = 0, mcpu = (0, 0), num_write_not_needed = 0
    Slot0: 00000000 00000000
    Slot1: 00000000 00000002
    Slot2: 00000000 00000000
    Slot3: 00000000 00000000
    Slot4: 00000000 00000000
    Slot5: 00000000 00000000
    Slot6: 00000000 00000000
```

```
    Slot7: 00000000 00000000
    Slot8: 00000000 00000000
    Slot9: 00000000 00000000
    Slot10: 00000000 00000000
    Slot11: 00000000 00000000
    Slot12: 00000000 00000000
    Slot13: 00000000 00000000
    Slot14: 00000000 00000000
    Slot15: 00000000 00000000
    Slot16: 00000000 00000000
    Slot17: 00000000 00000000
    Slot18: 00000000 00000000
    Slot19: 00000000 00000000
    Slot20: 00000000 00000000
    Slot21: 00000000 00000000
    Slot22: 00000000 00000000
    Slot23: 00000000 00000000
    Slot24: 00000000 00000000
    Slot25: 00000000 00000000
    Slot26: 00000000 00000000
    Slot27: 00000000 00000000
    Slot28: 00000000 00000000
    Slot29: 00000000 00000000
    Slot30: 00000000 00000000
    Slot31: 00000000 00000000
    Slot32: 00000000 00000000
    Slot33: 00000000 00000000
**********************(dm statsram pram <slot/port> <index>) output*********************************
(STATSRAM entry 0x03ff5b): pkt cnt: 217243, byte cnt: 32151964
```

History

Release version	Command history
5.9.00	This command was introduced.

show cam-detail-ip

Displays Content Addressable Memory (CAM) programming information for a specific Layer 3 CAM flow entry.

Syntax

show cam-detail-ip *slot/port ip_address/mask*

Parameters

slot/port

Specifies the LP module slot and port number.

ip_address/mask

Specifies IP address and mask of the Layer 3 PRAM entry.

Modes

Privileged EXEC mode.

Usage Guidelines

Use this command to retrieve and display Layer 3 CAM or Parameter Random Access Memory (PRAM) flow entry information without using a separate sequence of debugging commands. The command eliminates the need to remember indices information required to capture Layer 3 flow information by doing all the work in the back-end. The command only uses the network IP address and mask to read and display information for a specific PRAM entry.

The command is supported only on the Line Processor (LP) module. The command is supported only for IPv4 CAM or PRAM flow entry. IPv6 CAM or PRAM is not supported. The output from the command displays only default Virtual Routing and Forwarding (VRF) flow information.

NOTE

The command is supported on Brocade NetIron XMR Series and Brocade MLX Series devices.

Examples

The **show cam-detail-ip** command displays the following information on 2/2 with address 1.1.1.1/24:

```
device# show cam-detail-ip 2/2 1.1.1.1/24
**********************(show cam ip <ipaddr/mask>) output*****************************************
LP Index    IP Address         MAC            Age IFL/ Out IF PRAM
   (Hex)                                        VLAN        (Hex)
2  01a8da(R) 1.1.1.0/24         0024.3892.4c01 Dis 1    2/2    3ff62
**********************(dm cam [<interface> <index>]) output***************************************
(CAM 0x0001a8da left): 0.0.0.0/255.255.255.255
(CAM 0x0001a8da right): 1.1.1.0/255.255.255.0
**********************(dm cam2pram <interface> <index>) output*********************************
(CAM2PRAM entry 0x0351b4): 0003ffbb cam_idx: 0x0001a8da
(CAM2PRAM entry 0x0351b5 [MAC SA or Right IP]): 0003ff62
**********************(dm pram <interface> <index> ip) output***********************************
PRAM 0x3ff62 255[01770000:00000002:00000024:38924c01]128
             127[60008003:00000000:0400000d:00190200]0
************************PRAM IP entry **********************
DA HIGH          0x0024     Replacement DA (high 2 bytes)
DA LOW           0x38924c01 Replacement DA (low 4 bytes)
VLAN_ID          0001       Replacement VLAN ID
MULTICAST_VLAN   0          Set multicast flag in packet header
REPLACE_VLAN_ID  1          Use replacement VLAN ID
SPA_DISCARD_PKT  0          If 1, allow RPF to discard the packet
MTU_CHECK      1            If 1, enforce mtu check
REPLACE_DA       1          Use replacement DA
IGNORE_SPA_MASK  0          If 1, Ignore SPA mask
MONITOR          0          Copy packet to MONITOR port
CPU              0          Packet must be copied to CPU
DISCARD INVLD    0          Discard if lookup invalid
DISCARD PACKET   0          Force packet to be discarded
USE FID          1          Use FID from this PRAM entry
USE QOS ID       0          Use QOS ID for rate limiting
INNER VLAN VALID    0        Inner Vlan Valid
QOS ID           0x00       QOS rate limiting ID
VALID            0x000000d  Per-port entry valid
FID              0x0019     Forwarding ID
TRUNK ADJUST     0          Adjust FID based on trunk index
PRIORITY_FORCE   0
PRIORITY         0
FWD_COMMAND      2          L3 hardware forwarding command
USE TOS ID       0          Use replacement TOS
TOS ID           0x000      TOS replacement
IGNORE ACLRES    0          Ignore ACL lookup
VLAN ID     0000             Replacement Inner VLAN ID
PRAM TYPE        0
TRUNK ID         0
NEXTHOP ROUTER INDEX          0x00000000
TNNL_MTU_CHECK_LENGTH         1500
SRC_IPV4_ADDR/SPA MASK        0x00000002
GRE_TNNL_INGRESS              0
GRE_TNNL_ENGRESS              0
GRE_ENFORCE_SESSION_CHECK     0
6_TO_4_TNNL_INGRESS           0
6_TO_4_TNNL_EGRESS            0
6_TO_4_ENFORCE_SESSION_CHECK  0
TNNL_OUTER_TOS                0
REPLACE INNER VLAN            0
**********************(dm statsram pram <slot/port> <index>) output*********************************
(STATSRAM entry 0x3ff62): pkt cnt: 118298, byte cnt: 1750810
```

History

Release version	Command history
5.9.00	This command was introduced.

show cam ifl

Displays CAM interface entries..

Syntax

show cam ifl *slot*/*port*

Parameters

slot port

Displays CAM interface entries for the specified port.

Modes

Privileged EXEC mode.

Usage Guidelines

Use this command to display IPv4 interface CAM entries, including local (port+VLAN+IP) and remote (VC+IP) entries.

Command Output

The **show cam ifl** command displays the following information:

TABLE 9 show cam ifl output

Output field	Description
Slot	Slot-number
Index (Hex)	Shows the row number of this entry in the IP route table.
Port	Port-number
Outer VLAN	Shows path
Inner VLAN	Shows channel
PRAM (Hex	Shows the ACL PRAM entries.
IFL ID	Same as VPN-ID in IPVPN CAM
IPv4/v6 Routing	Shows whether IPv4 or IPv6 is enabled or disabled on the interface

Examples

The following examples displays CAM entries for interface 1/1.

```
device#show cam ifl 1/1
Slot Index    Port  Outer VLAN Inner VLAN PRAM    IFL ID IPV4/V6
     (Hex)                               (Hex)          Routing
4    0061ffd 1/2   1          0          001ffd 4097    0/0
4    0061fff 1/1   1          0          001fff 4097    1/0
```

To add VRF to VE.

```
Brocade(config)# vlan 22
Brocade(config-vlan-22)# tagged ethernet 1/7
Brocade(config-vlan-22)# router-interface ve 22
Brocade(config-vlan-22)# exit
Brocade(config)# interface ve 22
Brocade(config-vrf-22)# vrf forwarding blue
Brocade(config-vrf-22)# ip address 10.0.0.22/24
Brocade(config-vrf-22)# exit

device# show cam ifl 1/7
Slot Index   Port  Outer     VLAN     Inner VLAN     PRAM       IFL ID      IPV4/V6
     (Hex)                                  (Hex)                                                  Routing
1    0061fff 1/7   22              0                                          001fff     4097
1/0
```

show cam ipvpn

Displays CAM VPN entries.

Syntax

show cam ipvn *slot*/*port*

Parameters

slot port

Displays CAM VPN entries for the specified port.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display IPv4 VPN CAM entries, including local (port+VLAN+IP) and remote (VC+IP) entries.

Command Output

The **show cam ipvpn** command displays the following information:

TABLE 10 show cam ipvpn output

Output field	Description
LP	Shows the number of the interface module.
Index (Hex)	Shows the row number of this entry in the IP route table.
IP Address	Shows the IP address of the interface.
In Port	Shows the port number.
In VLAN	Shows the VLAN number.
VPNID	Shows VPNID in the display.
In VC Lb	Shows VC label.
MAC	Shows the MAC address of the interface.
Age	Shows whether the age is enabled or disabled.
IFL VLAN	Shows the VLAN to which the port belongs.
IF	Shows the state of outgoing interface action.
PRAM (Hex)	Shows the ACL PRAM entries.

Examples

The following example displays CAM entries for slot 1, port 7.

```
device# show cam ipvpn 1/7

LP Index IP Address                              In    In   VPNID In     MAC           Age
IFL/ IF                 PRAM
   (Hex)                                    Port  VLAN       VC
Lb                                                  VLAN                    (Hex)
1  308fa 10.0.0.0/32                     N/A   N/A  4097  N/A    N/A               Dis
N/A  Drop       000a8
1  308fb 10.0.0.255/32                      N/A           N/A  4097      N/A        N/A
Dis               N/A      Mgmt           000a7
1  308fc 10.0.0.22/32                    N/A   N/A  4097      N/A        N/A           Dis           N/
A      Mgmt       000a6
1  308fd 192.168.1.0/32          N/A       N/A      4097  N/A    N/A           Dis           N/A
Drop       000a5
1  308fe 192.168.1.255/32N/A   N/A  4097  N/A    N/A           Dis           N/A  Mgmt   000a4
1  308ff 192.168.1.1/32          N/A   N/A  4097  N/A    N/A           Dis           N/A  Mgmt   000a3
1  3e566 10.0.0.0/24                        N/A   N/A  4097  N/A    N/A           Dis           N/A
CPU    000a9
1  3e567 192.168.1.0/24      N/A   N/A  4097  N/A    N/A           Dis           N/A  CPU    000a1


To add VRF to VE.
Brocade(config)# vlan 22
Brocade(config-vlan-22)# tagged ethe 1/7
Brocade(config-vlan-22)# router-interface ve 22
Brocade(config-vlan-22)# exit
Brocade(config)# interface ve 22
Brocade(config-vif-22)# vrf forwarding blue
Brocade(config-vif-22)# ip address 10.0.0.22/24
Brocade(config-vif-22)# exit

Brocade# show cam ipvpn slot/port
```

show cam uda

Provides the details of the User Defined ACL (UDA) ACL CAM entry.

Syntax

show cam { **uda** } *slot/port*

Parameters

slot/port

Specifies the selected slot and port.

Modes

EXEC mode

Examples

The following example displays the output of the command.

```
device(config)# show cam  uda 1/1
LP Index  VLAN UDA0      UDA1      UDA2      UDA3     Port  Action   PRAM
   (Hex)                                                          (Hex)
1  057bfe 0    11223344  44556677  aabbccdd  0        1     Drop     7ff67
1  057c00 0    11223344  44556677  aabbccdd  0     0     Pass     7ff64
1  057c02 0    11223344  44556677  aabb      3333  0     Pass     7ff63
1  057c04 0    11223344  6677      aabb      aabb  0     Pass     7ff62
```

History

Release version	Command history
5.9.00	This command was introduced.

show cluster

Displays information about the Multi-Chassis Trunking (MCT) clusters of the peer and client states.

Syntax

show cluster [*cluster ID* [**ccp** | **client** [*client RBridge ID* | *client name* | **disabled**] | **client-health-check** | **l2vpn-peer** | **peer** | **vll**] | *cluster name* [**ccp** | **client** [*client RBridge ID* | *client name* | **disabled**] | **client-health-check** | **l2vpn-peer** | **peer** | **vll**] | **ccp** [**buffered_messages** | **peer**] | **config** [**begin** | **exclude** | **include**]]

show cluster

Parameters

cluster ID
Specifies the cluster ID.

ccp
Specifies the MCT Cluster Communication Protocol (CCP) for the chosen cluster ID or cluster name.

client
Specifies the cluster client information for the chosen cluster ID or cluster name.

client RBridge ID
Specifies the client RBridge ID.

client name
Specifies the cluster client name.

disabled
Shows the MCT spoke PW state for CCEP ports.

client-health-check
Specifies the cluster client health check information for the chosen cluster ID or cluster name.

l2vpn-peer
Specifies the cluster L2VPN peer information for the chosen cluster ID or cluster name.

peer
Specifies the cluster peer information for the chosen cluster ID or cluster name.

vll
Specifies the cluster virtual leased line (VLL) information for the chosen cluster ID or cluster name.

cluster name
Specifies the cluster name.

ccp
Specifies the MCT CCP information.

buffered_messages
Specifies the number of buffered CCP messages.

peer
Specifies the CCP peer information.

config
Specifies the MCT cluster configuration information.

begin
Specifies the output modifier by starting with the first matching line.

exclude
Specifies the output modifier by excluding the matching lines.

include
Specifies the output modifier by including the matching lines.

Modes

User EXEC mode

Global configuration mode

Usage guidelines

Information about the finite state machine (FSM) states that appear in the **show cluster** command output is provided in the following table.

Output field	Description
Admin Up	With the CCP up, a client reaches this state when both local and remote MCT client configurations are deployed by way of the command line interface and the corresponding ports on both local and remote MCT peers are down.
Remote Up	With the CCP up, a client reaches this state on a peer when the ports belonging to the client are down on the local device and are up on the remote MCT peer.
Local Up	With the CCP up, a client reaches this state on an MCT peer when the ports belonging to the client reach the forwarding state in that device and the corresponding ports of this client in the remote MCT peer are down.
Up	With the CCP up, a client reaches this state when both the local and remote ports belonging to the client are up and are in the forwarding state.

Examples

The following example displays the peer and client state cluster information.

```
device# show cluster
Cluster CLUSTER-1 2000
==================
Rbridge Id: 35535, Session Vlan: 2001, Keep-Alive Vlan: 301
Cluster State: Deploy
Client Isolation Mode: Loose
Configured Member Vlan Range: 2 to 2000 2002 to 4090
Active Member Vlan Range: 2 to 3 21 to 148 201 404 to 445 501 to 508 2010 3511 to
3574 4021 to 4025 4051 4070 4080 4087 4090
ICL Info:
---------
Name Port Trunk
ICL-1 2/1 6
Peer Info:
----------
Peer IP: 1.1.1.1, Peer Rbridge Id: 1, ICL: ICL-1
KeepAlive Interval: 50 , Hold Time: 300, Fast Failover
Active Vlan Range: 2 to 3 21 to 148 201 404 to 445 501 to 508 2010 3511 to 3574
4021 to 4025 4051 4070 4080 4087 4090
Peer State: CCP Up (Up Time: 0 days:19 hr:24 min: 8 sec)
 Client Info:
 ------------
 Name    Rbridge-id     Config     Port  Trunk FSM-State
 client-1   222        Deployed   1/2     3   Up
 client-2   22        Deployed   1/40     -   Up
```

The following example displays MCT cluster information when the MCT admin state is up.

```
device(config)# cluster TOR 1
device(config-cluster-TOR)# show cluster

Cluster TOR 1
=============
Rbridge Id: 2, Session Vlan: 4090
Cluster State: Deploy
Clients State: All client ports are administratively disabled
Client Isolation Mode: Loose
Cluster Mac Sync Mode: Enable, Mac sync Timer: 15 Min
Client Health Check Mode: Dynamic, Health Check Timer: 60 Sec
Configured Member Vlan Range: 2
Active Member Vlan Range: 2
Total Clients Configured : 2 ( Deployed Clients: 2)

 ICL Info:
 ---------
 Name                                                            Port  Trunk
 TOR                                                             1/9   1

 Peer Info:
 ----------
 Peer IP: 1.1.1.1, Peer Rbridge Id: 1, ICL: TOR
 KeepAlive Interval: 30 , Hold Time: 90, Fast Failover
 Active Vlan Range:  2
 Peer State: CCP Up (Up Time:   0 days: 0 hr:13 min:18 sec)

 Client Info:
 ------------
 Name    Rbridge-id     Config     Port  Trunk FSM-State
 client-1   100        Deployed   1/6     3   Admin Up
 client-2   200        Deployed   1/3     2   Admin Up
```

The following example displays MCT cluster information when the MCT remote state is up.

```
device(config)# cluster TOR 1
device(config-cluster-TOR)# client client-2
device(config-cluster-TOR-client-client-2)# show cluster

Cluster TOR 1
=============
Rbridge Id: 1, Session Vlan: 4090
Cluster State: Deploy
Client Isolation Mode: Loose
Configured Member Vlan Range: 2
Active Member Vlan Range: 2
Total Clients Configured : 2 ( Deployed Clients: 2)

 ICL Info:
 ---------
 Name                                                              Port  Trunk
 TOR                                                               1/9   1

 Peer Info:
 ----------
 Peer IP: 1.1.1.2, Peer Rbridge Id: 2, ICL: TOR
 KeepAlive Interval: 30 , Hold Time: 90, Fast Failover
 Active Vlan Range:  2
 Peer State: CCP Up (Up Time:   0 days: 0 hr:13 min: 8 sec)

 Client Info:
 ------------
 Name                  Rbridge-id Config     Port  Trunk FSM-State
 client-1              100        Deployed   1/3     2   Admin Up
 client-2              200        Deployed   1/6     3   Remote Up
```

The following example displays MCT cluster information when the MCT local state is up.

```
device(config)# cluster TOR 1
device(config-cluster-TOR)# show cluster
Cluster TOR 1
=============
Rbridge Id: 2, Session Vlan: 4090
Cluster State: Deploy
Client Isolation Mode: Loose
Configured Member Vlan Range: 2
Active Member Vlan Range: 2
Total Clients Configured : 2 ( Deployed Clients: 2)

 ICL Info:
 ---------
 Name                                     Port  Trunk
 TOR                                      1/9   1

 Peer Info:
 ----------
 Peer IP: 1.1.1.1, Peer Rbridge Id: 1, ICL: TOR
 KeepAlive Interval: 30 , Hold Time: 90, Fast Failover
 Active Vlan Range:  2
 Peer State: CCP Up (Up Time:   0 days: 0 hr:13 min:18 sec)

 Client Info:
 ------------
 Name               Rbridge-id Config     Port  Trunk FSM-State
 client-1           100        Deployed   1/6     3   Admin Up
 client-2           200        Deployed   1/3     2   Local Up
```

The following example displays cluster client information when the MCT spoke pseudowire (PW) state is down for the L2VPN MCT Cluster Client Edge Port (CCEP).

```
device(config)# show cluster 1 client disabled

 Name              Rbridge-id Config     Port  Trunk FSM-State    SpokePW-state
 R3                100        Deployed   3/3     3   Remote Up     Down
```

The following example displays the peer and client state cluster information and also identifies the LACP delay configured time of 5 seconds.

```
device#show cluster
Cluster mct 1
=============
Rbridge Id: 100, Session Vlan: 99
Cluster State: Deploy
Early sync of CCEP-UP info to MCT node enabled
lacp delay configured 5
Client Isolation Mode: Loose
Configured Member Vlan Range: 10
Active Member Vlan Range: 10
Total Clients Configured : 1 ( Deployed Clients: 1)

 ICL Info:
 ---------
 Name                                Port  Trunk
 icl                                  2/6   2

 Peer Info:
 ----------
 Peer IP: 1.1.1.2, Peer Rbridge Id: 200, ICL: icl
 KeepAlive Interval: 30 , Hold Time: 90, Fast Failover
 Active Vlan Range:  10
 Peer State: CCP Up (Up Time:   0 days: 0 hr:19 min:12 sec)

 Client Info:
 ------------
 Name               Rbridge-id    Config     Port  Trunk FSM-State
 switch bridge        10           Deployed   3/13    3    Up
```

History

Release version	Command history
5.4.00	This command was introduced.
5.9.00	This command was modified to include information about relevant FSM states.
6.0.00	This command was modified to include the **disabled** option for the **show cluster client** command. The command was also modified to include the LACP delay configured time value in the command output.

show configuration

Displays the router, switch, or firewall's current configuration.

Syntax

show configuration

Modes

EXEC mode.

Usage Guidelines

The outbound-fec filter configuration parameter now records in the startup or running configuration. It also now displays the name of the prefix-list configured in the LDP for outbound FEC filtering.

The outbound-fec filter configuration parameter is recorded in the startup or running configuration.

This command operates in all modes.

Examples

The following example displays output containing additional information indicating configured link protection:

```
device> show mpls conf
router mpls
  ……
lsp 1
  to 44.44.44.44
  adaptive
  frr
    link-protection
  enable
```

The following example displays output when there is no request for link protection:

```
device> show mpls conf
router mpls
  ……
 lsp 1
  to 44.44.44.44
  adaptive
  frr
  enable
```

History

Release	Command history
5.6.00	The outbound-fec filter configuration parameter is recorded in the startup or running configuration. The output of this command now contains additional information indication link protection is configured.

show cpu histogram

Displays task CPU usage information, including the percentage, and total percentage of the CPU utilization of a task histogram at 1, 5, and 10 second average duration.

Syntax

show cpu histogram { **hold** | **wait** | **interrupt** | **timer** } [**above** *threshold-value* | **noclear** | **taskname** *name*]

show cpu histogram { **util-10s** | **util-1s** | **util-5s** } [**above** *threshold-value* | **noclear** | **taskname** *name*]

show cpu histogram { **util-all-10s** | **util-all-1s** | **util-all-5s** } [**above** *threshold-value* | **noclear**]

Parameters

hold
Specifies the display of task hold time information.

wait
Specifies the display of task wait time information.

interrupt
Specifies the display of task user-interrupt usage information.

timer
Specifies the display of task sys-timer time usage information.

util-10s
Specifies the CPU utilization per task histogram at a 10 second average duration.

util-1s
Specifies the CPU utilization per task histogram at a 1 second average duration.

util-5s
Specifies the CPU utilization per task histogram at a 5 second average duration.

util-all-10s
Specifies the total CPU utilization of a task histogram at a 10 second average duration.

util-all-1s
Specifies the total CPU utilization of a task histogram at a 1 second average duration.

util-all-5s
Specifies the total CPU utilization of a task histogram at a 5 second average duration.

above *threshold-value*
Specifies the display of histogram information for tasks whose maximum hold time is above the specified value.

noclear
Specifies that histogram data should not be cleared after display. By default, information is cleared on read.

taskname *name*
Specifies the display of histogram information for a specific task.

Modes

User EXEC mode

Usage Guidelines

Use the command to display the task CPU usage information.

Use the **show cpu histogram**{ **util-10s** | **util-1s** | **util-5s** } command to display the CPU percentage of a task histogram utilizing high CPU conditions at 1, 5, and 10 second durations.

To display the total CPU unitization of a task histogram at 1, 5, and 10 second average duration, use the **show cpu histogram** { **util-all-10s** | **util-all-1s** | **util-all-5s** } command. This command is supported on the management module and the interface module. The CPU percent utilization and time stamps are displayed for the durations.

Tasks that may use high CPU utilization include packet burst in the interface module, multiple protocols flapping at the same time, a protocol task in a wrong state that keeps the CPU busy, and high route processing that causes high CPU conditions in the management module and interface module CPUs.

Command Output

The **show cpu histogram** command displays the following information:

Output field	Description
No of bucket	The task run time that is divided into interval buckets. For example, bucket 1(0-50ms), bucket2 (50-100ms), and bucket3(100-150ms).
Bucket Granularity	The bucket granularity is 5%. Each bucket contains values within 5% of range. For example, bucket 1 contains values 0-4, bucket 2 contains values 5-9, and so on.
Last Cleared at	The time at which the values are cleared last.
No of Task	The total number of tasks running in the system at a time.
Task Name	The name of the task displayed.
BktNum	The bucket number -1,2, or 3 that corresponds with the value it belongs to.
Bkt Value (%)	The time range of the bucket.
No of Time	The number of times the value in the bucket range is utilizing CPU. For example, task, sfm_mgr, was using the CPU in the range of 10-15, at 83 times.
CPU Util Total (%)	The total CPU utilization of a task.
Util Time Max	The maximum CPU utilization value of a bucket.
Time	The time stamp of the most recent CPU utilization for a particular task.

Examples

The following example displays task hold time information:

```
device# show cpu histogram hold
HISTOGRAM CPU HISTOGRAM INFO
----------------------------
 No of Bucket       : 51
 Bucket Granularity : 10 ms
 Last cleared at    : 2012.07.10-07:29:20.704
 No of Task         : 67
Task Name  Bkt     Bkt      No of Time   HoldTime   HoldTime                  Time
           Num     Time(ms)              Total(s)    Max(ms)
-------------------------------------------------------------------------------
ip_rx       1      000-010          4    .000463     .201  2012.07.10-07:29:20.701
vlan        1      000-010          1    .000025     .025  2012.07.10-07:29:20.700
mac_mgr     1      000-010          1    .000010     .010  2012.07.10-07:29:20.701
mrp         1      000-010          1    .000025     .025  2012.07.10-07:29:20.700
erp         1      000-010          1    .000025     .025  2012.07.10-07:29:20.700
mxrp        1      000-010          1    .000009     .009  2012.07.10-07:29:20.700
rtm         1      000-010          1    .000062     .062  2012.07.10-07:29:20.700
rtm6        1      000-010          1    .000091     .091  2012.07.10-07:29:20.700
ip_tx       1      000-010          1    .000207     .207  2012.07.10-07:29:20.700
l2vpn       1      000-010          1    .000018     .018  2012.07.10-07:29:20.701
ospf        1      000-010          1    .000046     .046  2012.07.10-07:29:20.700
isis        1      000-010          1    .000009     .009  2012.07.10-07:29:20.700
mcast       1      000-010          1    .000017     .017  2012.07.10-07:29:20.700
ospf6       1      000-010          1    .000012     .012  2012.07.10-07:29:20.700
mcast6      1      000-010          1    .000012     .012  2012.07.10-07:29:20.700
web         1      000-010          1    .000029     .029  2012.07.10-07:29:20.700
lacp        1      000-010          1    .000013     .013  2012.07.10-07:29:20.700
loop_detect 1      000-010          1    .000009     .009  2012.07.10-07:29:20.701
cluster_mgr 1      000-010          1    .000011     .011  2012.07.10-07:29:20.701
telnet_0    1      000-010          4       .003        3  2012.07.10-07:29:20.672
-------------------------------------------------------------------------------
```

The following example displays the CPU utilization of a task histogram at a 5 second average duration.

```
device# show cpu histogram util-5s
HISTOGRAM CPU UTIL PER TASK INFO (5sec average)
-----------------------------------------------
 No of Bucket       : 21
 Bucket Granularity : 5%
 Last cleared at    : 2014.09.04-18:18:39.607
 No of Task         : 72
Task Name        Bkt     Bkt      No of Time        CPU       Util                    Time
                 Num     Value(%)              Total(%)      Max(%)
-------------------------------------------------------------------------------------------
$flash             1      000-005          4          4          4  2014.09.10-01:08:29.500
$flash             2      005-010         17          7          7  2014.09.14-05:28:22.450
main               1      000-005          1         17          1  2014.09.04-18:18:44.350
ip_rx              1      000-005         18          1          1  2014.09.14-21:03:19.850
ip_rx              2      005-010          1         37          7  2014.09.05-02:00:13.050
console            1      000-005          2          7          1  2014.09.15-11:32:08.400
console            2      005-010          1         17          8  2014.09.04-18:18:44.350
```

History

Release	Command History
05.5.00	This command was introduced.

show cpu histogram sequence

Displays sequential execution of CPU task information.

Syntax

show cpu histogram sequence [**taskname** *name* | **above** *threshold-value* | **trace**]

Parameters

sequence

Specifies the display of sequential execution of CPU task information.

taskname *name*

Specifies the display of histogram information for a specific CPU task.

above *threshold-value*

Specifies the display of histogram information for CPU tasks whose maximum hold time is above the specified value.

trace

Specifies the display of high CPU condition task trace information.

Modes

User EXEC mode

Examples

The follow example displays sequential execution of CPU task information:

```
device# show cpu histogram sequence
HISTOGRAM TASK SEQUENCE INFO
----------------------------
 THRESHOLD  : 10 ms
 DURATION   : 30 s
----------------------------
Seq No Task Name    Context  HoldTime   Start Time     End Time       Date
                             Max (ms)
-------------------------------------------------------------------------------
     1 snms         TASK           16 07:33:08.790 07:33:08.806 2012.07.10
     2 snms         TASK           16 07:33:08.772 07:33:08.789 2012.07.10
     3 snms         TASK           17 07:33:08.755 07:33:08.772 2012.07.10
     4 snms         TASK           16 07:23:08.790 07:23:08.806 2012.07.10
     5 snms         TASK           16 07:23:08.772 07:23:08.789 2012.07.10
     6 snms         TASK           17 07:23:08.755 07:23:08.772 2012.07.10
     7 snms         TASK           16 07:13:08.790 07:13:08.806 2012.07.10
     8 snms         TASK           16 07:13:08.772 07:13:08.789 2012.07.10
     9 snms         TASK           17 07:13:08.755 07:13:08.772 2012.07.10
    10 snms         TASK           16 07:03:08.790 07:03:08.806 2012.07.10
    11 snms         TASK           16 07:03:08.772 07:03:08.789 2012.07.10
    12 snms         TASK           17 07:03:08.755 07:03:08.772 2012.07.10
    13 snms         TASK           16 06:53:08.790 06:53:08.806 2012.07.10
    14 telnet_0     TASK           50 09:51:50.091 09:51:50.142 2012.07.05
    15 telnet_0     TASK           50 09:51:35.184 09:51:35.234 2012.07.05
    16 console      TASK           50 09:51:11.451 09:51:11.501 2012.07.05
    17 telnet_0     TASK           50 09:47:01.459 09:47:01.509 2012.07.05
    18 console      TASK           52 09:46:32.443 09:46:32.496 2012.07.05
    19 mpls         TIMER          12 09:46:32.428 09:46:32.441 2012.07.05
    20 telnet_0     TASK           54 09:46:03.018 09:46:03.072 2012.07.05
    21 telnet_0     TASK           52 09:44:31.749 09:44:31.802 2012.07.05
    22 telnet_0     TASK           50 09:44:17.984 09:44:18.034 2012.07.05
    23 telnet_0     TASK           50 09:43:43.638 09:43:43.689 2012.07.05
    34 telnet_0     TASK           12 09:43:43.623 09:43:43.636 2012.07.05
    35 telnet_0     TASK           54 09:43:20.669 09:43:20.724 2012.07.05
    36 snms         TASK           16 09:43:08.740 09:43:08.756 2012.07.05
    37 snms         TASK           16 09:43:08.723 09:43:08.740 2012.07.05
-------------------------------------------------------------------------------
```

History

Release	Command History
R05.5.00	This command was introduced

show dot1x-mka group

Shows details for the specified MACsec Key Agreement (MKA) groups configured on this device, or for a designated MKA group.

Syntax

show dot1x-mka group *group-name*

Parameters

group-name

Limits the group configuration displayed to the named MKA group.

Modes

EXEC or Privileged EXEC mode

Command Output

The **show dot1x-mka group** command displays the following information:

Output field	Description
dot1x-mka group	The configuration details that follow are for the specified MACsec MKA group.
key-server-priority	The key server priority value used by MKA protocol for electing the key server.
macsec cipher-suite gcm-aes-128 or macsec cipher-suite gcm-aes-128 integrity-only	MACsec transmissions are encrypted. or ICV checking only is performed.
macsec confidentiality-offset	The byte offset used for encrypted data is set to the value shown. Allowable values are 0, 30 (the first 30 bytes of data are not encrypted), and 50 (the first 50 bytes of data are not encrypted).
macsec frame-validation {check | discard}	Indicates whether the MACsec frame header is checked and what action is taken for invalid frames (counted or discarded).
macsec replay-protection {strict | out-of-order window-size *size*}	Replay protection is enabled. The type of protection is shown as strict (discard any frame received out of sequence) or as allowing receipt of out-of-sequence frames within the specified window.
Capability	

Examples

The following example lists the configuration details for MKA group test1.

```
Brocade(config-dot1x-mka)#show dot1x-mka group group1
Brocade Group name group1
  Key Server Priority     : 16
  Cipher Suite            : gcm-aes-128
  Capability              : Integrity, Confidentiality with offset
  Confidentiality Offset  : 0
  Frame Validation        : strict
  Replay Protection       : strict
```

History

Release version	Command history
5.8.00	This command was introduced.

show dot1x-mka config

Shows the MACsec Key Agreement (MKA) configuration for the device.

Syntax

show dot1x-mka config

Modes

User EXEC mode

Usage Guidelines

Default configuration is not displayed when this command is executed.

Command Output

The **show dot1x-mka config** command displays the following information:

Output field	Description
dot1x-mka-enable	MACsec is enabled on the device.
enable-mka ethernet *slot/port*	The ethernet interfaces specified are enabled for MACsec.
mka-cfg-group *group-name*	The configuration details that follow are for the named MACsec MKA group.
key-server-priority *value*	The key server priority value used by MKA protocol for electing the key server.
macsec confidentiality-offset *value*	The byte offset used for encrypted data is set to the value shown. Allowable values are 30 (the first 30 bytes of data are not encrypted), and 50 (the first 50 bytes of data are not encrypted).
macsec frame-validation { check | discard }	For transmissions between MKA group members, indicates whether the MACsec frame header is checked and what action is taken for invalid frames (counted or discarded).
macsec-replay protection { strict | out-of-order window-size *value* }	Replay protection is enabled. The type of protection is shown as strict (discard any frame received out of sequence) or as allowing receipt of out-of-sequence frames within the specified window.
pre-shared-key *value* key-name *value*	The pre-shared key is set to this value and name for the MKA configuration group. Both key and name are hexadecimal strings.

Examples

The following example displays MACsec configuration information on Brocade device with MACsec enabled.

```
Brocade(config-dot1x-mka)#show dot1x-mka config
dot1x-mka-enable
  mka-cfg-group group1
    key-server-priority 20
    macsec frame-validation check
    macsec confidentiality-offset 30
    macsec replay-protection out-of-order window-size 100
  mka-cfg-group group2

  enable-mka ethernet 1/1 to ethernet 1/9
    mka-cfg-group    group1
    pre-shared-key 0102030405060708090A0B0C0D0E0F10 key-name 11223344
  enable-mka ethernet 1/10
    mka-cfg-group    group1
    pre-shared-key 0505030405060708090A0B0C0D0E0F10 key-name 55667788
```

History

Release version	Command history
5.8.00	This command was introduced.

show dot1x-mka sessions brief

Displays a brief summary of all MACsec Key Agreement (MKA) sessions on the device.

Syntax

show dot1x-mka sessions brief

Modes

User EXEC mode

Command Output

The **show dot1x-mka sessions** command with the **brief** option displays the following information:

Output field	Description
Port	Designates the interface for which MACsec information is listed (by device, slot, and port).
Link-Status	Indicates whether the link is up or down.
MKA-Status	Indicates whether a secure channel has been established.
Key-Server	Indicates whether the interface is operating as a key-server.
Negotiated Capability	Indicates MACsec parameters negotiated on the designated interface.

Examples

In the following example, all enabled MKA interfaces on the device are listed, along with configured parameters and current status.

```
device(config-dot1x-mka)# show dot1x-mka sessions brief

Port    Link-Status  Secured  Key-Server  Negotiated Capability
----    -----------  -------  ----------  ---------------------

4/2     Up           Yes      Yes         Integrity, Confidentiality with offset 0
4/3     Up           Yes      Yes         Integrity, Confidentiality with offset 0
4/4     Up           Yes      Yes         Integrity, Confidentiality with offset 0
4/7     Up           Yes      Yes         Integrity, Confidentiality with offset 0
4/11    Up           Yes      Yes         Integrity, Confidentiality with offset 0
4/12    Up           Yes      Yes         Integrity, Confidentiality with offset 0
4/17    Up           Yes      Yes         Integrity, Confidentiality with offset 0
4/18    Up           Yes      Yes         Integrity, Confidentiality with offset 0
```

History

Release version	Command history
5.8.00	This command was introduced.

show dot1x-mka sessions ethernet

Displays a summary of all MACsec Key Agreement (MKA) sessions on the device.

Syntax

show dot1x-mka sessions [**ethernet** *slot* **/** *port*]

Parameters

ethernet *slot* **/** *port*

Displays MKA sessions that are active on a specified Ethernet interface. The Ethernet interface is specified by slot on the device, and interface on the slot.

Modes

User EXEC mode

Command Output

The **show dot1x-mka sessions** command with the **ethernet** interface options displays the following information:

Output field	Description
Interface	The information that follows applies to the designated interface.
DOT1X-MKA Enabled (Yes, No)	Indicates whether MKA is enabled for the designated interface.
DOT1X-MKA Active (Yes, No)	Indicates whether MKA is active on the interface.
Key Server (Yes, No)	Indicates whether the MKA key-server is active over the interface.
Configuration Status:	**The following fields describe the MKA configuration applied to the interface.**
Enabled (Yes, No)	Indicates whether MACsec is currently enabled.
Group name	MKA configuration group that has been associated with the interface.
Capability (Integrity and or confidentiality)	Indicates whether ICV checks are being performed on MACsec frames and whether encryption is being applied.
Confidentiality offset	Specifies the offset value set.
Desired (Yes, No)	Indicates whether port is interested in securing the communication using MACsec.
Protection (Yes, No)	Indicates whether replay protection is applied to the interface.
Validation	Indicates whether frames received are being checked for valid MACsec headers.
Replay Protection (Strict, Out of Order)	Indicates that replay protection is configured and whether frames must be received in exact order or within an allowable window.
Replay Protection Size	Indicates the allowable window size within which frames may be received.
Cipher Suite (GCM-AES-128)	Specifies the cipher suite used for ICV checking, encryption, and decryption.
Authenticator	
Key Server Priority	Specifies the key-server priority configured on the interface.
Algorithm Agility	
CAK NAME	
Secure Channel Information(SCI)	**The following fields describe a secure channel established on this interface.**

Output field	Description
Actor SCI	Provides the hexadecimal value of the Secure Channel Identifier for this channel.
Actor Priority	
Key Server SCI	
Key Server Priority	
Logon Status:	
Enabled	
Authenticated	
Secured	
Failed	
Latest KI, KN and AN Information:	
Latest KI	
Tx Key Number	
Rx Key Number	
Tx Association Number	
Rx Association Number	
Participant Information:	
SCI	
Key Identifier	
Member Identifier	Provides the MACsec number assigned to the MKA peer.
Message Number	Provides the Message Number contained in Hello packets from this MKA peer. Hello packets are exchanged to determine peer status, MACsec capabilities, and SAK Key Identifier.
CKN	
Key Length(in bytes)	
Secure Channel Information:	
No. of Peers (Live and Potential)	
Latest SAK Status	Indicates the Secure Association Key (SAK) state.
Negotiated Capability (Integrity and or Confidentiality with offset)	Indicates whether ICV checking, encryption, and a confidentiality offset have been applied on the secure channel. (The negotiated capability may differ from parameters configured on the interface when it does not have key-server status.)

The output fields that follow provide information on actual and potential MACsec peer interfaces

Output field	Description
State (Live or Potential)	Indicates whether the peer is considered a live peer or a potential peer for MKA protocol.
Member Identifier	Designates the peer by its Member Identifier, a hexadecimal value.
Message Number	Provides the Message Number that appears in Hello packets from the designated peer interface as a hexadecimal value.
SCI	Provides the peer's Secure Channel Identifier.
Priority	Provides the key-server priority configured on the peer interface.

Examples

The following example lists MKA sessions that are active on Ethernet interface 4/1, with configuration details for each active interface.

```
Brocade(config)#show dot1x-mka sessions ethernet 4/1


Interface                : 4/1

  DOT1X-MKA Enabled      : Yes
  DOT1X-MKA Active       : Yes

Configuration Status:
  Group Name             : 1
  Capability             : Integrity, Confidentiality with offset
  Confidentiality offset : 0

  Desired                : Yes
  Protection             : Yes
  Validation             : Strict
  Replay Protection      : None
  Replay Protection Size : 0
  Cipher Suite           : GCM-AES-128

  Authenticator          : No
  Key Server Priority    : 16
  Algorithm Agility      : 80C201

  CAK NAME               : 11223344

SCI Information:
  Actor SCI              : 0024388f6b900001
  Actor Priority         : 16
  Key Server SCI         : 0024388f6b900001
  Key Server Priority    : 16

MKA Status:
  Enabled                : Yes
  Authenticated          : No
  Secured                : Yes
  Failed                 : No

Latest KI, KN and AN Information:
  Latest KI              : 42b4d71d520263cad8727d9100000001
  Tx Key Number          : 1
  Rx Key Number          : 0
  Tx Association Number  : 0
  Rx Association Number  : 0

Participant Information:
  SCI                    : 0024388f6b900001
  Key Identifier         : 1
  Member Identifier      : 42b4d71d520263cad8727d91
  Message Number         : 3491
  CKN Name               : 11223344
  Key Length(in bytes)   : 16

Secure Channel Information:
  No. of Peers (Live and Potential)  : 1
  Latest SAK Status                : Rx & TX
  Negotiated Capability            : Integrity, Confidentiality with offset 0


Peer Information(Live and Potential):
State Member Identifier       Message Number  SCI               Priority   Capability
----- ----------------        --------------  ----------------   --------  ----------
Live  66dfa9b5037a9c7aa8b5c71e  3490          0024389e2d300001  16        2
```

History

Release version	Command history
5.8.00	This command was introduced.

show dot1x-mka statistics

Displays current MACsec Key Agreement (MKA) statistics on the interface.

Syntax

show dot1x-mka statistics ethernet *slot*/*port*

Parameters

ethernet *slot*/*port*

Ethernet interface for which MKA statistics are to be displayed. The interface is designated by a slot on the device and interface on the slot.

Modes

EXEC or Privileged EXEC mode

Usage Guidelines

It is recommended that you use the **clear dot1x-mka statistics** command to clear results of the previous **show dot1x-mka statistics** command before re-executing it.

Command Output

The **show dot1x-mka statistics** command displays the following information:

Output field	Description
Interface (slot/port)	The output fields describe MACsec activity for the designated interface.
MKA in Pkts	MKA protocol packets received
MKA in SAK Pkts	MKA protocol packets received containing a SAK
MKA in Bad Pkts	MKA protocol packets received that are bad
MKA in Bad ICV Pkts	MKA protocol packets received with a bad ICV
MKA in Mismatch Pkts	MKA protocol packets received with mismatched CAK
MKA out Pkts	MKA protocol packets transmitted
MKA out SAK Pkts	MKA protocol packets transmitted containing a SAK

Examples

The following example shows MKA statistics for Ethernet interface 3/2, which is transmitting and receiving MACsec frames.

```
Brocade(config)# show dot1x-mka statistics ethernet 3/2

Interface                : 3/2

MKA in Pkts              : 89858
MKA in SAK Pkts          : 0
MKA in Bad Pkts          : 0
MKA in Bad ICV Pkts      : 0
MKA in Mismatch Pkts     : 0
MKA out Pkts             : 90225
MKA out SAK Pkts         : 192
```

History

Release version	Command history
5.8.00	This command was introduced.

show egress-truncate

Displays the configuration details for the egress-truncate command.

Syntax

show egress-truncate

show egress-truncate interface *slot/port*

Parameters

interface

Displays the configuration of the ports in a slot determined by the *slot/port* variable.

Modes

This command operates under all modes.

Command Output

The **show egress-truncate** *interface* command displays the following information:

Output field	Description
SlotNo	The slot number where egress-truncate has been applied.
Device-id	The device ID of where egress-truncate has been applied.
Size	The configured size of the egress truncated packet.
Status	The status (enabled or disabled) for the specified interface.

Examples

The following example displays the **show egress-truncate** command:

```
device#show egress-truncate
SlotNo Device-id   Size      Status
1        1        100        Enabled
2        2        90        Enabled
3        1        64        Enabled
Enabled Ports:  e 10/1
device#
```

The following example displays the **show egress-truncate interface** command

```
device#show egress-truncate interface 10/1
 Device status : Enabled
 Egress Truncate Packet Size:200
 Port Status: Enabled
device#
```

History

Release version	Command history
05.9.00	This command was introduced.

show flow-ctrl

This command provide a consolidated and system wide flow-control status at the port, MAC/XPP and TM level.

Syntax

show flow-ctrl { **status** | **all**|**slot** slot number|**ethernet**[**slot**slot number|**port**port number]}

Parameters

all

dumps the high-level flow control information from all the slots in the chassis.

slot

dumps the flow control information for all the ports for the specifiled slot.

ethernet

dumps the flow control information for the specified port or slot.

status

dumps the flow control status (enabled or disabled) and ignores the pause RX status.

Modes

Privilege exec

Usage Guidelines

On Darter (BR-MLX-10Gx24-DM) or ports on Darter (BR-MLX-10Gx24-DM), the flow control information dump at the MAC contains only the ongoing egress MAC flow control assertion" information. NP flow control details will not be available

Examples

Following is a sample output for ethernet interface level command.

```
device# show flow-ctrl ethernet 1/1
Port 1/1
InPauseFrames:                    123
Egress MAC flow control assertions (latched):     Yes (0x01000000)
Egress MAC flow control assertions (ongoing):     Yes (0x00000100)
NP Info for Ports 1/1 - ¼
Egress NP flow control assertions (latched):     Yes (0x01000000)
Egress NP flow control assertions (ongoing):     Yes (0x00000100)
Ingress NP flow control assertions (latched):     Yes (0x00010000)
Ingress NP flow control assertions (ongoing):     No
TM Info for Ports 1/1 - 1/4
Flow control at the egress queue interface:         No
  CFC (Centralized Flow Control) Status 0:              No
  CFC (Centralized Flow Control) Status 1:              No
  CFC (Centralized Flow Control) Status 2:              No
```

Following is a sample output for slot level command. Assume the slot is a 8x10G module.

```
device# show flow-ctrl slot 1
Port 1/1
InPauseFrames:                      123
Egress MAC flow control assertions (latched):     Yes (0x01000000)
Egress MAC flow control assertions (ongoing):     Yes (0x00000100)
Port 1/2
InPauseFrames:                      0
Egress MAC flow control assertions (latched):     No
Egress MAC flow control assertions (ongoing):     No
…
…
<for ports till 1/8>
NP Info for Ports 1/1 - ¼
Egress NP flow control assertions (latched):     Yes (0x01000000)
Egress NP flow control assertions (ongoing):     Yes (0x00000100)

Ingress NP flow control assertions (latched):     Yes (0x00010000)
Ingress NP flow control assertions (ongoing):     No
TM Info for Ports 1/1 - 1/4
Flow control at the egress queue interface:         No
  CFC (Centralized Flow Control) Status 0:              No
  CFC (Centralized Flow Control) Status 1:              No
  CFC (Centralized Flow Control) Status 2:              No

NP Info for Ports 1/5 - 1/8
Egress NP flow control assertions (latched):     Yes (0x01000000)
Egress NP flow control assertions (ongoing):     Yes (0x00000100)
Ingress NP flow control assertions (latched):     Yes (0x00010000)
Ingress NP flow control assertions (ongoing):     No
TM Info for Ports 1/5 - 1/8
Flow control at the egress queue interface:         No
  CFC (Centralized Flow Control) Status 0:              No
  CFC (Centralized Flow Control) Status 1:              No
  CFC (Centralized Flow Control) Status 2:              No
```

History

Release version	Command history
6.1	The option "status" is introduced to the command.

show ikev2 policy

Displays configuration information about Internet Key Exchange version 2 (IKEv2) policies.

Syntax

show ikev2 policy [*policy-name*]

Parameters

policy-name

Specifies the name of an IKEv2 policy.

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

When a policy is not specified, this command displays information about all IKEv2 policies.

Command Output

The **show ikev2 policy** command displays the following information:

Output field	Description
Name	The name of an IKEv2 policy.
vrf	The front-door VRF (fvrf) to match for the policy.
Local address/Mask	The local IP address to match for the policy.
Proposal	The IKEv2 proposal that is configured for the policy.

Examples

The following example displays information about all configured IKEv2 policies.

```
device# show ikev2 policy

   Name                : ike_policy_red
   vrf                 : Default
   Local address/Mask  : 0.0.0.0/0.0.0.0
   Proposal            : ike_proposal_red

   Name                : ikev2-default-policy
   vrf                 : Default
   Proposal            : ikev2-default-proposal
```

History

Release version	Command history
5.8.00	This command was introduced.

show ikev2 profile

Displays information about the configured IKEv2 profile.

Syntax

show ikev2 profile *profile-name*

Parameters

profile-name

Specifies the IKEv2 profile name.

Modes

Privileged EXEC mode

Examples

The following example displays **show ikev2 profile** command output.

```
device# show ikev2 profile

 IKEv2 profile       : ike_profile_blue
 Auth Profile        : auth_blue
 Match criteria      :
  IKE session vrf    : default-vrf
  Local:
   address 1.2.10.1
  Remote:
   address 1.2.10.2
 Local identifier    : address 1.2.10.1
 Remote identifier   : address 1.2.10.2
 Local auth method: pki
 Remote auth method(s): pki
 Lifetime          : 86400 sec
 keepalive check   : disabled


 IKEv2 profile     : ike_profile_green
 Auth Profile: auth_green
 Match criteria:
  IKE session vrf  : default-vrf
  Local:
   address 1.2.10.1
  Remote:
   address 1.2.10.2    fdqn RTB_green
 Local identifier  : address 1.2.10.1
 Remote identifier : address 1.2.10.2
 Local auth method: pki
 Remote auth method(s): pki
 Lifetime          : 1440 minutes
 keepalive check   : disabled
```

History

Release version	Command history
05.8.00	This command was introduced.

show ikev2 proposal

Displays configuration information about Internet Key Exchange version 2 (IKEv2) proposals.

Syntax

show ikev2 proposal [*name*]

Parameters

name

Specifies the name of an IKEv2 proposal.

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

When an IKEv2 proposal is not specified, this command displays configuration information for all IKEv2 proposals.

Command Output

The **show ikev2 proposal** command displays the following information:

Output field	Description
Name	The name of an IKEv2 proposal.
Encryption	The encryption algorithms that are configured for the proposal.
Integrity	The integrity algorithms that are configured for the proposal.
PRF	The pseudorandom function algorithms that are configured for the proposal.
DH Group	The Diffie-Hellman groups that are configured for the proposal.

Examples

The following example shows how to display information about the IKEv2 proposal configuration.

```
device# show ikev2 proposal

     Name       : ikev2-default-proposal
     Encryption : AES-CBC-256
     Integrity  : sha384
     PRF        : sha384
     DH Group   : 384_ECP/Group 20
```

History

Release version	Command history
5.8.00	This command was introduced.

show ikev2 sa

Displays information about the current IKEv2 Security Associations (SA) that exist between the specified local and remote interfaces. This command supports IPsec IPv4 and IPv6.

Syntax

show ikev2 sa [**spi-index** | **fvrf***vrf-name* | **local** [*address* | *ipv6-address*] | **remote** *address*] [**detail**]

Parameters

spi-index
(Optional) Specifies the IKEv2 Security Parameter Index (SPI) value.

fvrf *vrf-name*
(Optional) Specifies the front VRF name.

local *address*
(Optional) Specifies the IPv4 address of the local interface.

local *ipv6-address*
(Optional) Specifies the IPv6 address of the local interface.

remote *address*
(Optional) Specifies the IP address of the remote interface.

detail
(Optional) Specifies to include details of the IKEv2 SA in the output.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not include the optional **detail** parameter, only the basic information about the SA is included in the output. If you want to view information about the interface role (initiator or responder), SPI indexes, or the selected IKEv2 policy or profile, make sure you include the **detail** parameter.

Examples

These examples are for IPsec IPv4.

The following example shows output for command **show ikev2 sa** for the SA between local interface 1.2.10.1 and remote interface 1.2.10.2. The **detail** keyword was not included.

```
device# show ikev2 sa

tnl-id     local                remote               Status      vrf(i) vrf(f)
-------------------------------------------------------------------------------
tnl 2      1.2.10.1/500         1.2.10.2/500         rdy  Blue   Default
```

The following example shows output for command **show ikev2 sa detail** for the SA between local interface 1.2.10.1 and remote interface 1.2.10.2. The **detail** keyword was included.

```
device# show ikev2 sa detail

tnl-id     local                remote               status      vrf(i) vrf(f)
-------------------------------------------------------------------------------
2          1.2.10.1/500         1.2.10.2/500         rdy  Blue   Default
      Role               : Initiator
      Local SPI          : 0xf327d32cd0df9106     Remote SPI: 0x34bec986ed6c232e
      Ike Profile        : mlx2_1
      Ike Policy         : mlx2_1
      Auth Proposal      : def-ike-auth-prop
```

History

Release version	Command history
05.8.00	This command was introduced.
05.9.00	This command was modified to add support for IPsec IPv6.

show ikev2 session

Displays information about the configured IKEv2 profile.

Syntax

show ikev2 session *local-spi-id* [**detail**]

Parameters

local-spi-id

Specifies the local SPI ID value.

detail

Specifies the detailed description of the IKEv2 profile.

Modes

Privileged EXEC mode

Examples

The following example displays **show ikev2 session** command output.

```
device# show ikev2 session

IKE count:1, CHILD count:1
Tunnel-id  Local                Remote               Status      vrf(i) vrf(f)
------------------------------------------------------------------------------
Tnl 2          1.2.10.1/500          1.2.10.2/500          rdy|in-use  Blue   Default
child sa:
 id 1
       local selector  0.0.0.0/0 - 255.255.255.255/65535
       remote selector 0.0.0.0/0 - 255.255.255.255/65535
       ESP spi in/out: 0x0000004b/0x0000005e
       Encryption: aes-gcm-256, ICV Size: 16 octects, Esp_hmac: null
       Authetication: null  DH Group:none , Mode: tunnel
```

The following example displays **show ikev2 session detailed** command output.

```
device# show ikev2 session detailed

IKE count:1, CHILD count:1

Tunnel-id  Local                Remote               Status      vrf(p) vrf(f)
------------------------------------------------------------------------------
2          1.2.10.1/500         1.2.10.2/500         rdy|in-use  Blue   Default
      Encr: aes-cbc-256, Hash: sha384, DH Grp:384_ECP/Group 20, Auth: not supported
    Life/Active Time: 86400/361 sec
    Status Description: Negotiation done
       Local spi: f7c029048eb25082       Remote spi: 56b8735e2f6afbde
       Local id : address 1.2.45.2       Remote id : address 1.2.45.1
       No Exchange in Progress
       Next Request Message id=29
          Total Keepalive sent: 0     Total Keepalive Received: 0
       Time Past Since Last Msg: 60

child sa:
 id 1
       local selector  0.0.0.0/0 - 255.255.255.255/65535
       remote selector 0.0.0.0/0 - 255.255.255.255/65535
       ESP spi in/out: 0x0000004b/0x0000005e
       Encryption: aes-gcm-256, ICV Size: 16 octects, Esp_hmac: null
       Authetication: null  DH Group:none , Mode: tunnel
```

History

Release version	Command history
05.8.00	This command was introduced.

show ikev2 statistics

Displays statistical information about Internet Key Exchange version 2 (IKEv2).

Syntax

show ikev2 statistics

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

Command Output

The **show ikev2 statistics** command displays the following information:

Output field		Description
Total IKEv2 SA Count active		The total number of IKEv2 security associations (SAs) in an active state.
Incoming IKEv2 Requests		The number of IKEv2 SAs (accepted and rejected) initiated by the peer device.
Outgoing IKEv2 Requests		The number of IKEv2 SAs initiated by the local device.
	Accepted	The total number of outgoing IKEv2 SAs that were accepted.
	Rejected	The total number of outgoing IKEv2 SAs that were rejected.
	Rejected due to no cookie	The total number of outgoing IKEv2 SAs that were rejected due to no cookie.
IKEv2 Packet Statistics		
	Total Packets Received	The total number of packets received.
	Total Packets Transmitted	The total number of packets transmitted.
	Total Packets Retransmitted	The total number of packets retransmitted.
	Total Failed Transmission	The total number of packets where transmission failed.
	Total Pending Packets	The total number of packets to be transmitted.
	Total Buffer Failed	The total number of packets where transmission failed due to a buffer issue.
	Total Keepalive Received	The total number of IKEv2 keepalive messages received.
	Total Keepalive Transmitted	The total number of IKEv2 keepalive messages transmitted.
IKEv2 Error Statistics		
	Unsupported Payload	The total number of IKEv2 packets received with an unsupported payload.
	Invalid IKE SPI	The total number of IKEv2 packets received with an invalid security parameter index (SPI).
	Invalid Version	The total number of IKEv2 packets received with an invalid version.
	Invalid Syntax	The total number of IKEv2 packets received with invalid syntax.
	Negotiation Timeout	The total number of IKEv2 sessions deleted due to dead peer detection (DPD) or negotiation timeouts.
	No Policy	The total number of IKEv2 sessions deleted or rejected due to a policy issue.

Output field		Description
	No Protection Suite	The total number of IKEv2 sessions deleted or rejected due to a protection suite issue.
	Policy Error	The total number of IKEv2 sessions deleted or rejected due to policy error.
	IKE Packet Error	The total number of IKEv2 or IPsec packets received with a packet error.
	Discard Policy	The total number of IKEv2 or IPsec sessions deleted or rejected due to a policy error or mismatch.
	Proposal Mismatch	The total number of IKEv2 or IPsec packets sent or received with a proposal mismatch.
	Invalid Selectors	The total number of IKEv2 or IPsec packets sent or received with invalid selectors.
	Internal Error	The total number of IKEv2 or IPsec packets sent or received with an internal error.
	SA Overflow	The total number of times the maximum SA count was reached.
	IKE SA Overflow	The number of times the maximum IKEv2 SA count was reached.
	IPSEC SA Overflow	The number of times the maximum IPsec SA count was reached.
	Authentication Failed	The total number of IKEv2 or IPsec packets sent or received when authentication failed.
	Others	The total number of IKEv2 or IPsec packets sent or received with other error types.
	Number of HW-SPI Add write	The number of times the creation of an IPsec SPI was written to the hardware.
	Number of HW-SPI Delete	The number of times the deletion of an IPsec SPI was written to the hardware.

Examples

The following example displays **show ikev2 statistics** command output.

```
device#show ikev2 statistics
Total IKEv2 SA Count   : 1 active: 1 negotiating: 0
Incoming IKEv2 Requests: 0 accepted: 0 rejected: 0
Outgoing IKEv2 Requests: 1 accepted: 1 rejected: 0
Rejected IKEv2 Requests: 0
Incoming IKEV2 Cookie Challenged Requests: 0
accepted: 0 rejected: 0 rejected no cookie: 0
IKEv2  Packet Statistics:
    Total Packets Received     : 57
    Total  Packets Transmitted : 57
    Total Packets Retransmitted: 0
    Total Keepalive Received   : 10
    Total Keepalive Transmitted: 10
IKEv2 Error Statistics:
    Unsupported Payload   : 0     Invalid IKE SPI  : 0
    Invalid Version       : 0     Invalid Syntax   : 0
    Proposal Mismatch     : 0     Invalid Selectors: 0
    Authentication Failed : 0     Others           : 0
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00a	This command was modified to include output fields for extended IKEv2 counters.

show interface ethernet

Displays the interfaces associated with the specified port.

Syntax

show interface ethernet *slot/port-number*

Parameters

slot/port-number

Specifies the slot and port bumber.

Modes

Any command mode.

Examples

The following example displays information pertaining to an Ethernet interface.

```
device# show interface ethernet
100GigabitEthernet2/1 is empty, line protocol is down
  Port state change time: May 10 07:17:16  (13 days 13:02:18 ago)
  Loopback: None
  STP Root Guard is disabled, STP BPDU Guard is disabled
  Hardware is 100GigabitEthernet, address is 0024.3890.3b30 (bia 0024.3890.3b30)
  Configured speed 100Gbit, actual unknown, configured duplex fdx, actual unknown
  Member of VLAN 1 (untagged), port is in untagged mode, port state is Disabled
  STP configured to ON, Priority is level0, flow control enabled
  Priority force disabled, Drop precedence level 0, Drop precedence force disabled
  dhcp-snooping-trust configured to OFF
  mirror disabled, monitor disabled
  LACP BPDU Forwarding:Disabled
  LLDP BPDU Forwarding:Disabled
  UDA Offsets :Disabled
  GTP de-encapsulation: Enabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  Port is not enabled to receive all vlan packets for pbr
  MTU 1548 bytes, encapsulation ethernet
  Configured BW is 100000000 kbps
  Openflow: Disabled, Openflow Index 49
  Cluster L2 protocol forwarding enabled
  300 second input rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  300 second output rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts, 0 unicasts
  0 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  NP received 0 packets, Sent to TM 0 packets
  NP Ingress dropped 0 packets
  0 packets output, 0 bytes, 0 underruns
  Transmitted 0 broadcasts, 0 multicasts, 0 unicasts
  0 output errors, 0 collisions
  NP transmitted 0 packets, Received from TM 0 packets
```

The following example shows an output with the port-state-change time highlighted for port 3 on slot 1.

```
Brocade(config)#show interface ethernet 1/3
10GigabitEthernet1/3 is up, line protocol is down (LACP-BLOCKED)
  Port state change time: Jan 21 02:40:21,  (0 days, 00:07:16 ago)
  Loopback: None
  STP Root Guard is disabled, STP BPDU Guard is disabled
  Hardware is 10GigabitEthernet, address is 0024.38a4.3802 (bia 0024.38a4.3802)
  …
  NP transmitted 11115 packets, Received from TM 11115 packets
```

History

Release version	Command history
5.6.00	This command was introduced.
5.9.00	This command was modified to display Egress truncate status and configured size and port state change time.
6.1.0	This command output was updated to display the GTP de-encapsulation feature status.

show interfaces tunnel

Displays the IP addresses and unicast and multicast traffic counters for the specified IPv4 IPsec tunnel. This command cannot be used on IPv6 IPsec tunnels.

Syntax

show interfaces tunnel *num*

Parameters

num

Specifies the tunnel number.

Modes

User EXEC mode

Command Output

The **show interfaces tunnel** command displays the following information:

Output field	Description
Tunnel number	The number of the tunnel.
Tunnel source	The IP address of the interface that is configured as the source of the tunnel. IP packets are forwarded from this interface across the tunnel.
Tunnel destination	The IP address of the interface that is configured as the destination of the tunnel. IP packets forwarded from the tunnel source interface are received by this interface.
Tunnel mode	The specified tunnel mode for the tunnel. This indicates which version of IP (IPv4 or IPv6) has been enabled on the tunnel interface. NOTE The tunnel mode is always IPv4 when using this command (this command can only be used on IPv4 IPsec tunnels).
Port name	The specified name of the port. If a name was not specified, the output shows no port name.
Internet address	The IP address of the port. This is not the IP address of the tunnel source or destination.
Tunnel TOS	The value to write into the ToS byte in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 99, where 0 means a tunnel packet copies the ToS value from the packet being encapsulated (the passenger packet).
Tunnel TTL	The value to write into the TTL field in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 255, where 0 means a tunnel packet copies thevalue from the packet being encapsulated (the passenger packet). The default value is 255.
Tunnel MTU	This maximum size allowable for IP packets entering the tunnel. Packets that exceed the value you specify (or the default) are sent back to the source. The default value is 1480 bytes.
Tunnel vrf	
Forwarding vrf	
Tunnel protection profile	The name of the IPsec profile used to encapsulate and encrypt the IP packets being transmitted by the tunnel interface. A tunnel profile defines a set of encapsulation and encryption methods used to secure IP packets.

Output field	Description
Tunnel packet statistics	The following packet counts for **unicast** traffic on the tunnel: • **RxPkts:** The total number of IP packets received from the tunnel on the interface. • **TxPkts:** The total number of IP packets transmitted across the tunnel from the interface. • **RxBytes:** The total number of bytes received from the tunnel on the interface. (The total is for IP packets only.) • **TxBytes:** The total number of bytes transmitted across the tunnel from the interface. (The total is for IP packets only.)
Tunnel multicast packet statistics	The following packet counts for **multicast** traffic on the tunnel: • **RxMcPkts:** The total number of IP multicast packets received from the tunnel on the interface. • **TxMcPkts:** The total number of IP multicast packets transmitted across the tunnel from the interface.

Usage Guidelines

This command is restricted to showing data for IPv4 IPsec tunnels.

NOTE

If you want to view the same information for IPv6 IPsec tunnels, use the **show ipv6 interface tunnel** command.

Examples

The following example shows output for tunnel number 10.

```
device# show interfaces tunnel 10
Tunnel10 is IPSec port up, line protocol is up
  Hardware is Tunnel
  Tunnel source is 1.1.1.1
  Tunnel destination is 1.1.1.2
  Tunnel mode IPSec IPv4
  No port name
  Internet address is: 11.11.11.5/24
  Tunnel TOS 0, Tunnel TTL 255, Tunnel MTU 1431 bytes
  Tunnel vrf (IVRF): default-vrf
  Forwarding vrf(FVRF): default-vrf
  Tunnel protection profile: abcd
Tunnel Packet Statistics:
  RxPkts: 100            TxPkts: 11200
  RxBytes: 150            TxBytes: 12544
Tunnel Multicast Packet Statistics:
  RxMcPkts: 5394           TxMcPkts:  67
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00	This command was modified to include multicast packet statistics information for the tunnel.

show ip allow-src-multicast

Displays whether the packet drop for multicast IPv4 or IPv6 as the source IP address is enabled or disabled.

Syntax

show ip allow-src-multicast [**switched-only**]

Parameters

switched-only

Displays switched multicast traffic as the source IP address.

Modes

User EXEC mode

Command Output

The **show ip allow-src-multicast** command displays the following information.

Output field	Description
Disable packet drop for multicast IPv4/IPv6 as source IP	Displays whether the disable packet drop for multicast IPv4 or IPv6 addresses as the source IP address is enabled or disabled.
Disable packet drop for multicast switched traffic only	Displays the slot on which the disable packet drop for switched traffic only is enabled.

Examples

The following example displays the disable packet drop for multicast IPv4 or IPv6 addresses as source IP address in a disabled state.

```
device# show ip allow-src-multicast
  Disable packet drop for multicast ipv4/ipv6 as source ip:
  DISABLED
```

The following example displays the disabled packet drop for switched traffic only in an enabled state for slot 3.

```
device# show ip allow-src-multicast switched-only
 Disable packet drop for switched traffic only:
 ENABLED ON:
 Slot 3
```

History

Release version	Command history
5.9.00	This command was introduced.

show ip bgp

Displays entries in the IPv4 Border Gateway Protocol (BGP4) routing table.

Syntax

show ip bgp

show ip bgp *ip-addr* [*/prefix*]

show ip bgp *ip-addr* [*/prefix*] **longer-prefixes**

Parameters

ipv6-addr/prefix

IPv4 address and optional prefix.

longer-prefixes

Filters on prefixes equal to or greater than that specified by *prefix*.

Modes

User EXEC mode

Examples

This example displays sample output from the **show ip bgp** command.

```
device> show ip bgp

Total number of BGP Routes: 4
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
*>i 110.110.110.0/24   50.50.50.10                150        0      i
*x  110.110.110.0/24   20.20.20.10                100        0      200 i
*   110.110.110.0/24   30.30.30.10                100        0      300 i
*   110.110.110.0/24   40.40.40.10                100        0      400 i
```

This example displays sample output from the **show ip bgp** command when an IP address is specified.

```
device> show ip bgp 10.3.4.0

Number of BGP Routes matching display condition : 1
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        Metric LocPrf Weight Path
*>  10.3.4.0/24         192.168.4.106          100    0      65001 4355 1 1221 ?
       Last update to IP routing table: 0h11m38s, 1 path(s) installed:
         Gateway           Port
         192.168.2.1       2/1
       Route is advertised to 1 peers:
        10.20.20.2(65300)
```

show ip bgp attribute-entries

Displays BGP4 route-attribute entries that are stored in device memory.

Syntax

show ip bgp attribute-entries

Modes

User EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4 attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4 route-attribute entries that are stored in device memory.

Command Output

The **show ip bgp attribute-entries** command displays the following information:

Output field	Description
Total number of BGP4 Attribute Entries	The number of routes contained in this BGP4 route table.
Next Hop	The IP address of the next-hop device for routes that have this set of attributes.
Metric	The cost of the routes that have this set of attributes.
Origin	The source of the route information. The origin can be one of the following: • EGP - The routes with these attributes came to BGP4 through EGP. • IGP - The routes with these attributes came to BGP4 through IGP. • INCOMPLETE - The routes came from an origin other than one of the above. For example, they may have been redistributed from OSPF or RIP. When BGP4 compares multiple routes to a destination to select the best route, IGP is preferred over EGP and both are preferred over INCOMPLETE.
Originator	The originator of the route in a route reflector environment.
Cluster List	The route-reflector clusters through which this set of attributes has passed.
Aggregator	Aggregator information: • AS Number shows the AS in which the network information in the attribute set was aggregated. This value applies only to aggregated routes and is otherwise 0. • Router-ID shows the device that originated this aggregator.

Output field	Description
Atomic	Whether the network information in this set of attributes has been aggregated *and* this aggregation has resulted in information loss. • TRUE - Indicates information loss has occurred • FALSE - Indicates no information loss has occurred **NOTE** Information loss under these circumstances is a normal part of BGP4 and does not indicate an error.
Local Pref	The degree of preference for routes that use these attributes relative to other routes in the local AS.
Communities	The communities to which routes with these attributes belong.
AS Path	The autonomous systems through which routes with these attributes have passed. The local AS is shown in parentheses.

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: 18 (0)
1       Next Hop  :192.168.1.6        MED :1             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
        Extended Community: SOO 300000:3
        AS Path   :90000 80000 (length 11)
        Address: 0x10e4e0c4  Hash:489 (0x03028536), PeerIdx 0
        Links: 0x00000000, 0x00000000, nlri: 0x10f4804a
        Reference Counts: 1:0:1, Magic: 51
2       Next Hop  :192.168.1.5        Metric   :1         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
        Extended Community: RT 200000:2
        AS Path   :90000 75000 (length 11)
        Address: 0x10e4e062  Hash:545 (0x0301e8f6), PeerIdx 0
        Links: 0x00000000, 0x00000000, nlri: 0x10f47ff0
        Reference Counts: 1:0:1, Magic: 49
```

show ip bgp config

Displays active BGP4 configuration information.

Syntax

show ip bgp config

Modes

User EXEC mode

Examples

This example displays sample output from the **show ip bgp config** command.

```
device> show ip bgp config

router bgp
  local-as 200
neighbor 10.102.1.1 remote-as 200
neighbor 10.102.1.1 ebgp-multihop
neighbor 10.102.1.1 update-source loopback 1
neighbor 192.168.2.1 remote-as 100
neighbor 10.200.2.2 remote-as 400
neighbor 2001:db8::1:1 remote-as 200
neighbor 2001:db8::1:2 remote-as 400
neighbor 2001:db8::1 remote-as 300

address-family ipv4 unicast
no neighbor 2001:db8::1:1 activate
no neighbor 2001:db8::1:2 activate
no neighbor 2001:db8::1 activate
exit-address-family

address-family ipv4 multicast
exit-address-family

address-family ipv6 unicast
redistribute static
neighbor 2001:db8::1:1 activate
neighbor 2001:db8::1:2 activate
neighbor 2001:db8::1 activate
exit-address-family
end of BGP configuration
```

show ip bgp dampened-paths

Displays all BGP4 dampened routes.

Syntax

show ip bgp dampened-paths

Modes

User EXEC mode

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*]

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.

name

Name of an AS-path ACL or prefix list.

Modes

User EXEC mode

Examples

This example displays BGP4 filtered routes.

```
device> show ip bgp filtered-routes
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
       Prefix             Next Hop        MED       LocPrf     Weight Status
1      10.3.0.0/8          192.168.4.106              100        0      EF
         AS_PATH: 65001 4355 701 80
2      10.4.0.0/8          192.168.4.106              100        0      EF
         AS_PATH: 65001 4355 1
3      10.60.212.0/22      192.168.4.106              100        0      EF
         AS_PATH: 65001 4355 701 1 189
```

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-prefix**]

show ip bgp flap-statistics as-path-filter *name*

show ip bgp flap-statistics neighbor *ip-addr*

show ip bgp flap-statistics regular-expression *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.

as-path-filter *name*
Specifies an AS-path filter.

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

User EXEC mode

Command Output

The **show ip bgp flap-statistics** command displays the following information:

Output field	Description
Total number of flapping routes	The total number of routes in the BGP4 route table that have changed state and have been marked as flapping routes.

Output field	Description
Status code	Indicates the dampening status of the route, which can be one of the following: • > - This is the best route among those in the BGP4 route table to the route destination. • d - This route is currently dampened, and unusable. • h - The route has a history of flapping and is unreachable now. • * - The route has a history of flapping but is currently usable.
Network	The destination network of the route.
From	The neighbor that sent the route to the device.
Flaps	The number of flaps the route has experienced.
Since	The amount of time since the first flap of this route.
Reuse	The amount of time remaining until this route will be un-suppressed and can be used again.
Path	Shows the AS-path information for the route.

Examples

The following example displays route dampening statistics.

```
device> show ip bgp flap-statistics
Total number of flapping routes: 414
    Status Code  >:best d:damped h:history *:valid
    Network            From         Flaps Since    Reuse    Path
h>  10.50.206.0/23   10.90.213.77   1     0 :0 :13 0 :0 :0  65001 4355 1 701
h>  10.255.192.0/20  10.90.213.77   1     0 :0 :13 0 :0 :0  65001 4355 1 7018
h>  10.252.165.0/24  10.90.213.77   1     0 :0 :13 0 :0 :0  65001 4355 1 7018
h>  10.50.208.0/23   10.90.213.77   1     0 :0 :13 0 :0 :0  65001 4355 1 701
h>  10.33.0.0/16     10.90.213.77   1     0 :0 :13 0 :0 :0  65001 4355 1 701
*>  10.17.220.0/24   10.90.213.77   1     0 :1 :4  0 :0 :0  65001 4355 701 62
```

show ip bgp ipv6

Displays IPv6 unicast information.

Syntax

show ip bgp ipv6 neighbors

show ip bgp ipv6 neighbors *ip-addr* **advertised-routes** [**detail**] [*ipv6 address /mask*]

show ip bgp ipv6 neighbors *ip-addr* **flap-statistics**

show ip bgp ipv6 neighbors *ip-addr* **last-packet-with-error** [**decode**]

show ip bgp ipv6 neighbors *ip-addr* **received** [**prefix-filter**]

show ip bgp ipv6 neighbors *ip-addr* **received-routes** [**detail**]

show ip bgp ipv6 neighbors *ip-addr* **rib-out-routes** [**detail**] [*ipv6 address /mask*]

show ip bgp ipv6 neighbors *ip-addr* **routes**

show ip bgp ipv6 neighbors *ip-addr* **routes** { **best** | **not-installed-best** | **unreachable** }

show ip bgp ipv6 neighbors *ip-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** }

show ip bgp ipv6 neighbors *ip-addr* **routes-summary**

show ip bgp ipv6 neighbors last-packet-with-error

show ip bgp ipv6 neighbors routes-summary

show ip bgp ipv6 summary

Parameters

neighbors
Specifies a neighbor.

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

advertised-routes
Specifies the routes that the device has advertised to the neighbor during the current BGP4 session.

detail
Specifies detailed information.

ipv6 address /mask
Specifies an IPv6 address and mask.

flap-statistics
Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

last-packet-with-error
Specifies the last packet with an error.

decode
Decodes the last packet that contained an error from any of a device's neighbors.

received
Specifies Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

prefix-filter
Displays the results for ORFs that are prefix-based.

received-routes
Specifies all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

rib-out-routes
Displays information about the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

routes
Displays a variety of route information received in UPDATE messages from BGP4 neighbors.

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.

routes-summary
Displays all route information received in UPDATE messages from BGP4 neighbors.

summary
Displays summarized IPv6 unicast information.

Modes

User EXEC mode

Examples

The following example displays summarized IPv6 unicast information.

```
device> show ip bgp ipv6 summary
BGP4 Summary
Router ID: 10.1.1.1 Local AS Number: 1
Confederation Identifier: not configured
Confederation Peers:
Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
Number of Neighbors Configured: 1, UP: 1
Number of Routes Installed: 1, Uses 86 bytes
Number of Routes Advertising to All Neighbors: 0 (0 entries)
Number of Attribute Entries Installed: 1, Uses 90 bytes
Neighbor Address AS# State Time Rt:Accepted Filtered Sent ToSend
192.168.1.2 2 ESTAB 0h 1m51s 1 0 0 0
```

The following example displays IPv6 unicast device information with respect to IPv4 neighbors.

```
device(config-bgp)# show ip bgp ipv6 neighbors
Total number of BGP Neighbors: 1
1 IP Address: 192.168.1.2, AS: 2 (EBGP), RouterID: 10.1.1.2, VRF: default-vrf
State: ESTABLISHED, Time: 0h8m33s, KeepAliveTime: 60, HoldTime: 180
KeepAliveTimer Expire in 17 seconds, HoldTimer Expire in 135 seconds
UpdateSource: Loopback 1
RefreshCapability: Received
.......
Neighbor NLRI Negotiation:
Peer Negotiated IPV6 unicast capability
Peer configured for IPV6 unicast Routes
Neighbor ipv6 MPLS Label Capability Negotiation:
Neighbor AS4 Capability Negotiation:
TCP Connection state: ESTABLISHED, flags:00000033 (0,0)
```

show ip bgp neighbors

Displays configuration information and statistics for BGP4 neighbors of the device.

Syntax

show ip bgp neighbors [*ip-addr*]

show ip bgp neighbors last-packet-with-error

show ip bgp neighbors routes-summary

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

last-packet-with-error

Displays the last packet with an error.

routes-summary

Displays routes received, routes accepted, number of routes advertised by peer, and so on.

Modes

User EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Command Output

The **show ip bgp neighbors** command displays the following information:

Output field	Description
Total Number of BGP4 Neighbors	The number of BGP4 neighbors configured.
IP Address	The IP address of the neighbor.
AS	The AS the neighbor is in.
EBGP or IBGP	Whether the neighbor session is an IBGP session, an EBGP session, or a confederation EBGP session: • EBGP - The neighbor is in another AS. • EBGP_Confed - The neighbor is a member of another sub-AS in the same confederation. • IBGP - The neighbor is in the same AS.
RouterID	The neighbor device ID.
Description	The description you gave the neighbor when you configured it on the device.

Output field	Description
Local AS	The value (if any) of the Local AS configured.
State	The state of the session with the neighbor. The states are from the device perspective, not the neighbor perspective. The state values are based on the BGP4 state machine values described in RFC 1771 and can be one of the following for each device: • IDLE - The BGP4 process is waiting to be started. Usually, enabling BGP4 or establishing a neighbor session starts the BGP4 process. A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • ADMND - The neighbor has been administratively shut down. A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • CONNECT - BGP4 is waiting for the connection process for the TCP neighbor session to be completed. • ACTIVE - BGP4 is waiting for a TCP connection from the neighbor. NOTE If the state frequently changes between CONNECT and ACTIVE, there may be a problem with the TCP connection. • OPEN SENT - BGP4 is waiting for an Open message from the neighbor. • OPEN CONFIRM - BGP4 has received an OPEN message from the neighbor and is now waiting for either a KEEPALIVE or NOTIFICATION message. If the device receives a KEEPALIVE message from the neighbor, the state changes to Established. If the message is a NOTIFICATION, the state changes to Idle. • ESTABLISHED - BGP4 is ready to exchange UPDATE messages with the neighbor. If there is more BGP4 data in the TCP receiver queue, a plus sign (+) is also displayed. NOTE If you display information for the neighbor using the **show ip bgp neighbor***ip-addr* command, the TCP receiver queue value will be greater than 0.
Time	The amount of time this session has been in the current state.
KeepAliveTime	The keep alive time, which specifies how often this device sends keepalive messages to the neighbor.
HoldTime	The hold time, which specifies how many seconds the device will wait for a keepalive or update message from a BGP4 neighbor before deciding that the neighbor is not operational.
PeerGroup	The name of the peer group the neighbor is in, if applicable.
Multihop-EBGP	Whether this option is enabled for the neighbor.
RouteReflectorClient	Whether this option is enabled for the neighbor.
SendCommunity	Whether this option is enabled for the neighbor.
NextHopSelf	Whether this option is enabled for the neighbor.
DefaultOriginate	Whether this option is enabled for the neighbor.
MaximumPrefixLimit	Maximum number of prefixes the device will accept from this neighbor.

Output field	Description
RemovePrivateAs	Whether this option is enabled for the neighbor.
RefreshCapability	Whether this device has received confirmation from the neighbor that the neighbor supports the dynamic refresh capability.
CooperativeFilteringCapability	Whether the neighbor is enabled for cooperative route filtering.
Distribute-list	Lists the distribute list parameters, if configured.
Filter-list	Lists the filter list parameters, if configured.
Prefix-list	Lists the prefix list parameters, if configured.
Route-map	Lists the route map parameters, if configured.
Messages Sent	The number of messages this device has sent to the neighbor. The display shows statistics for the following message types: • Open • Update • KeepAlive • Notification • Refresh-Req
Messages Received	The number of messages this device has received from the neighbor. The message types are the same as for the Message Sent field.
Last Update Time	Lists the last time updates were sent and received for the following: • NLRIs • Withdraws
Last Connection Reset Reason	The reason the previous session with this neighbor ended. The reason can be one of the following: Reasons described in the BGP4 specifications: • Message Header Error • Connection Not Synchronized • Bad Message Length • Bad Message Type • OPEN Message Error • Unsupported Version Number • Bad Peer AS Number • Bad BGP4 Identifier • Unsupported Optional Parameter • Authentication Failure • Unacceptable Hold Time • Unsupported Capability • UPDATE Message Error • Malformed Attribute List • Unrecognized Well-known Attribute • Missing Well-known Attribute • Attribute Flags Error • Attribute Length Error • Invalid ORIGIN Attribute • Invalid NEXT_HOP Attribute • Optional Attribute Error • Invalid Network Field • Malformed AS_PATH

Output field	Description
	• Hold Timer Expired • Finite State Machine Error • Rcv Notification
Last Connection Reset Reason (cont.)	Reasons specific to the Brocade implementation: • Reset All Peer Sessions • User Reset Peer Session • Port State Down • Peer Removed • Peer Shutdown • Peer AS Number Change • Peer AS Confederation Change • TCP Connection KeepAlive Timeout • TCP Connection Closed by Remote • TCP Data Stream Error Detected
Notification Sent	If the device receives a NOTIFICATION message from the neighbor, the message contains an error code corresponding to one of the following errors. Some errors have subcodes that clarify the reason for the error. Where applicable, the subcode messages are listed underneath the error code messages. • Message Header Error: – Connection Not Synchronized – Bad Message Length – Bad Message Type – Unspecified • Open Message Error: – Unsupported Version – Bad Peer As – Bad BGP4 Identifier – Unsupported Optional Parameter – Authentication Failure – Unacceptable Hold Time – Unspecified • Update Message Error: – Malformed Attribute List – Unrecognized Attribute – Missing Attribute – Attribute Flag Error – Attribute Length Error – Invalid Origin Attribute – Invalid NextHop Attribute – Optional Attribute Error – Invalid Network Field – Malformed AS Path – Unspecified • Hold Timer Expired • Finite State Machine Error • Cease • Unspecified
Notification Received	Refer to details for the field Notification Sent.
TCP Connection state	The state of the connection with the neighbor. The connection can have one of the following states: • LISTEN - Waiting for a connection request.

Output field	Description
	• SYN-SENT - Waiting for a matching connection request after having sent a connection request. • SYN-RECEIVED - Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTABLISHED - Data can be sent and received over the connection. This is the normal operational state of the connection. • FIN-WAIT-1 - Waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent. • FIN-WAIT-2 - Waiting for a connection termination request from the remote TCP. • CLOSE-WAIT - Waiting for a connection termination request from the local user. • CLOSING - Waiting for a connection termination request acknowledgment from the remote TCP. • LAST-ACK - Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request). • TIME-WAIT - Waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request. • CLOSED - There is no connection state.
Byte Sent	The number of bytes sent.
Byte Received	The number of bytes received.
Local host	The IP address of the device.
Local port	The TCP port the device is using for the BGP4 TCP session with the neighbor.
Remote host	The IP address of the neighbor.
Remote port	The TCP port the neighbor is using for the BGP4 TCP session with the device.
ISentSeq	The initial send sequence number for the session.
SendNext	The next sequence number to be sent.
TotUnAck	The number of sequence numbers sent by the device that have not been acknowledged by the neighbor.
TotSent	The number of sequence numbers sent to the neighbor.
ReTrans	The number of sequence numbers that the device retransmitted because they were not acknowledged.
UnAckSeq	The current acknowledged sequence number.
IRcvSeq	The initial receive sequence number for the session.
RcvNext	The next sequence number expected from the neighbor.
SendWnd	The size of the send window.
TotalRcv	The number of sequence numbers received from the neighbor.
DupliRcv	The number of duplicate sequence numbers received from the neighbor.
RcvWnd	The size of the receive window.
SendQue	The number of sequence numbers in the send queue.

Output field	Description
RcvQue	The number of sequence numbers in the receive queue.
CngstWnd	The number of times the window has changed.

Examples

This example shows sample output from the show ip bgp neighbors command.

```
device> show ip bgp neighbors

    '+': Data in InQueue '>': Data in OutQueue '-': Clearing
    '*': Update Policy 'c': Group change 'p': Group change Pending
    'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1   IP Address: 60.60.60.20, AS: 200 (IBGP), RouterID: 60.60.60.20, VRF: default-vrf
    State: ESTABLISHED, Time: 4h3m28s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 0 seconds, HoldTimer Expire in 159 seconds
    Minimal Route Advertisement Interval: 0 seconds
       RefreshCapability: Received
    Address Family : IPV4 Unicast
       Configured with Add-Path(send receive)capability
       Received Add-Path (send receive)capability in open msg
       Negotiated Add-Path(send receive)capability
    Messages:    Open        Update      KeepAlive   Notification   Refresh-Req
       Sent    : 1           1           275         0              0
       Received: 1           1           275         0              0
    Last Update Time: NLRI       Withdraw          NLRI       Withdraw
                  Tx: 4h3m28s    ---           Rx: 4h3m28s    ---
```

This example shows sample output from the show ip bgp neighbors command when an IP address is specified.

```
device> show ip bgp neighbors 10.4.0.2
    Total number of BGP neighbors:
1   IP Address: 10.4.0.2, AS: 5 (EBGP), RouterID: 10.0.0.1
       Description: neighbor 10.4.0.2
    Local AS: 101
    State: ESTABLISHED, Time: 0h1m0s, KeepAliveTime: 0, HoldTime: 0
       PeerGroup: pg1
       Multihop-EBGP: yes, ttl: 1
       RouteReflectorClient: yes
       SendCommunity: yes
       NextHopSelf: yes
       DefaultOriginate: yes (default sent)
       MaximumPrefixLimit: 90000
       RemovePrivateAs: : yes
       RefreshCapability: Received
    Route Filter Policies:
       Distribute-list: (out) 20
       Filter-list: (in) 30
       Prefix-list: (in) pf1
       Route-map: (in) setnp1  (out) setnp2
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 1       1       1         0            0
       Received: 1       8       1         0            0
    Last Update Time: NLRI       Withdraw          NLRI       Withdraw
                  Tx: 0h0m59s    ---           Rx: 0h0m59s    ---
    Last Connection Reset Reason:Unknown
      Notification Sent:     Unspecified
      Notification Received: Unspecified
    TCP Connection state: ESTABLISHED
       Local host:  10.4.0.1, Local  Port: 179
       Remote host: 10.4.0.2, Remote Port: 8053
       ISentSeq:   52837276  SendNext:   52837392  TotUnAck:          0
       TotSent:         116  ReTrans:           0  UnAckSeq:   52837392
       IRcvSeq:  2155052043  RcvNext:  2155052536  SendWnd:       16384
       TotalRcv:        493  DupliRcv:          0  RcvWnd:        16384
       SendQue:           0  RcvQue:            0  CngstWnd:       1460
```

History

Release version	Command history
5.9.00	The command was modified. Description codes were added to display output.
6.0.0	This command was modified to include BGP add path configuration status.

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*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Specifies detailed information.

mask-bits

Number of mask bits in CIDR notation.

Modes

User EXEC mode

Examples

This example displays the routes the device has advertised to a specified neighbor.

```
device> show ip bgp neighbors 192.168.4.211 advertised-routes

       There are 2 routes advertised to neighbor 192.168.4.211
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST I:IBGP L:LOCAL
       Network        Next Hop        Metric  LocPrf   Weight   Status
1      10.102.0.0/24  192.168.2.102   12              32768    BL
2      10.200.1.0/24  192.168.2.102   0               32768    BL
```

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**

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

Modes

User EXEC mode

show ip bgp neighbors last-packet-with-error

Displays the last packets with an error from BGP4 neighbors of the device.

Syntax

show ip bgp neighbors *ip-addr* **last-packet-with-error** [**decode**]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

decode

Decodes the last packet that contained an error from any of a device's neighbors.

Modes

User EXEC mode

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** { **extended-community** | **prefix-filter** }

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

extended-community

Displays the results for ORFs that use the BGP Extended Community Attribute.

prefix-filter

Displays the results for ORFs that are prefix-based.

Modes

User EXEC mode

Examples

This example displays sample output for the **show ip bgp neighbors received** command when the **prefix-filter** keyword is used.

```
device> show ip bgp neighbor 10.10.10.1 received prefix-filter

ip prefix-list 10.10.10.1: 4 entries
     seq 5 permit 10.10.0.0/16 ge 18 le 28
     seq 10 permit 10.20.10.0/24
     seq 15 permit 10.0.0.0/8 le 32
     seq 20 permit 10.10.0.0/16 ge 18
```

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**]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays detailed route information.

Modes

User EXEC mode

Examples

This example displays the details of route updates for VRF instance "red".

```
device> show ip bgp neighbor 10.168.4.106 received-routes

       There are 97345 received routes from  neighbor 10.168.4.106
Searching for matching routes, use ^C to quit...
tatus A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTEREDtatus A:AGGREGATE B:BEST
b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
       Prefix              Next Hop        MED     LocPrf    Weight Status
1      10.3.0.0/8          10.168.4.106            100       0      BE
         AS_PATH: 65001 4355 701 8
2      10.4.0.0/8          10.168.4.106            100       0      BE
         AS_PATH: 65001 4355 1
3      10.60.212.0/22      10.168.4.106            100       0      BE
         AS_PATH: 65001 4355 701 1 189
4      10.6.0.0/8          10.168.4.106            100       0      BE
```

show ip bgp neighbors rib-out-routes

Displays information about the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

Syntax

show ip bgp neighbors *ip-addr* **rib-out-routes** [**detail**] [*ip-addr* [**/** *mask*]]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

last-packet-with-error

Displays the last packet with an error.

routes-summary

Displays routes received, routes accepted, number of routes advertised by peer, and so on.

Modes

User EXEC mode

Examples

This example shows information about the routes that the device either has most recently sent, or is about to send, to a specified neighbor and a specified destination network

```
device> show ip bgp neighbor 192.168.4.211 rib-out-routes 192.168.1.0/24

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST I:IBGP L:LOCAL
       Prefix             Next Hop        Metric     LocPrf     Weight Status
1      10.200.1.0/24       0.0.0.0         0          101         32768  BL
```

show ip bgp routes community

Displays BGP4 route information that is filtered by community and other options.

Syntax

show ip bgp routes community { *num* | *aa:nn* | **internet** | **local-as** | **no-advertise** | **no-export** }

Parameters

community

Displays routes filtered by a variety of communities.

num

Specifies a community number n the range from 1 to 4294967200.

aa:nn

Specifies an autonomous system-community number.

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.

Modes

User EXEC mode

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** }

show ip bgp neighbors *ip-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** }

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.

Modes

User EXEC mode

Examples

The following example shows sample output for the **show ip bgp neighbors routes** command.

```
device> show ip bgp neighbors 192.168.4.106 routes

       There are 97345 received routes from  neighbor 192.168.4.106
Searching for matching routes, use ^C to quit...
tatus A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTEREDtatus A:AGGREGATE B:BEST
b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
       Prefix             Next Hop        MED     LocPrf    Weight Status
1      10.3.0.0/8          192.168.4.106           100       0      BE
         AS_PATH: 65001 4355 701 8
2      10.4.0.0/8          192.168.4.106           100       0      BE
         AS_PATH: 65001 4355 1
3      10.60.212.0/22      192.168.4.106           100       0      BE
         AS_PATH: 65001 4355 701 1 189
4      10.6.0.0/8          192.168.4.106           100       0      BE
…
```

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**

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

Modes

User EXEC mode

Command Output

The **show ip bgp neighbors routes-summary** command displays the following information:

Output field	Description
IP Address	The IP address of the neighbor.
Routes Received	How many routes the device has received from the neighbor during the current BGP4 session: • Accepted or Installed - Number of received routes the device accepted and installed in the BGP4 route table. • Filtered or Kept - Number of routes that were filtered out, but were retained in memory for use by the soft reconfiguration feature. • Filtered - Number of received routes 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 IP Forwarding Table	The number of routes received from the neighbor that are the best BGP4 routes to their destinations, but were not installed in the IP route table because the device received better routes from other sources (such as OSPF, RIP, or static IP routes).
Unreachable Routes	The number of routes received from the neighbor that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next-hop.
History Routes	The number of routes that are down but are being retained for route flap dampening purposes.
NLRIs Received in Update Message	The number of routes received in Network Layer Reachability (NLRI) format in UPDATE messages: • Withdraws - Number of withdrawn routes the device has received. • Replacements - Number of replacement routes the device has received.

Output field	Description
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 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. • maxas-limit aspath - The number of route entries discarded because the AS path exceeded the configured maximum length or exceeded the internal memory limits. • Invalid Nexthop - The next-hop value was not acceptable. • Duplicated Originator_ID - The originator ID was the same as the local device ID. • Cluster_ID - The cluster list contained the local cluster ID, or the local device ID 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 queued to send to this neighbor. • To be Withdrawn - The number of NLRIs for withdrawing routes the device has queued 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 - Number of routes the device has sent to the neighbor to withdraw. • Replacements - 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 route information base (Adj-RIB-Out) for routes to be advertised.

Examples

The following example displays route summary information received in UPDATE messages.

```
device> show ip bgp neighbor 10.168.4.211 routes-summary

1   IP Address: 10.168.4.211
Routes Accepted/Installed:1,  Filtered/Kept:11,  Filtered:11
   Routes Selected as BEST Routes:1
      BEST Routes not Installed in IP Forwarding Table:0
   Unreachable Routes (no IGP Route for NEXTHOP):0
   History Routes:0

NLRIs Received in Update Message:24,  Withdraws:0 (0),  Replacements:1
   NLRIs Discarded due to
      Maximum Prefix Limit:0, AS Loop:0
      Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
      Duplicated Originator_ID:0, Cluster_ID:0

Routes Advertised:0,  To be Sent:0,  To be Withdrawn:0
NLRIs Sent in Update Message:0,  Withdraws:0,  Replacements:0

Peer Out of Memory Count for:
   Receiving Update Messages:0, Accepting Routes(NLRI):0
   Attributes:0, Outbound Routes(RIB-out):0
```

show ip bgp peer-group

Displays peer-group information.

Syntax

show ip bgp peer-group *peer-group-name*

Parameters

peer-group-name

Specifies a peer group name.

Modes

User EXEC mode

Usage Guidelines

Only the parameters that have values different from their defaults are listed.

Examples

This example shows sample output from the **show ip bgp peer-group** command.

```
device> show ip bgp peer-group STR
1   BGP peer-group is STR
      Address family : IPV4 Unicast
        activate
      Address family : IPV4 Multicast
        no activate
      Address family : IPV6 Unicast
        no activate
      Address family : IPV6 Multicast
        no activate
      Address family : VPNV4 Unicast
        no activate
      Address family : L2VPN VPLS
        no activate
    Members:
       IP Address: 10.1.1.1, AS: 5
```

show ip bgp routes

Displays statistics for the routes in the BGP4 route table of a device.

Syntax

show ip bgp routes [**detail**] [*num* | *ip-address/prefix* | **age** *num* | **as-path-access-list** *name* | **as-path-filter** *number* | **best** | **cidr-only** | **community-access-list** *name* | **community-filter** *number* | **community-reg-expression** *expression* | **local** | **neighbor** *ip-addr* | **nexthop** *ip-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**]

Parameters

detail
Displays detailed information.

num
Table entry at which the display starts. For example, if you want to list entries beginning with table entry 100, specify 100.

ip-address/prefix
Specifies an IP address and prefix.

age *num*
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).

as-path-filter *number*
Displays BGP4 route information that is filtered using the specified AS-path filter.

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.

community-filter *number*
Displays BGP4 route information that matches a specific community filter.

community-reg-expression *expression*
Displays BGP4 route information for an ordered community list regular expression.

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 a prefix list.

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.

Modes

User EXEC mode

Command Output

The **show ip bgp routes** command displays the following information:

Output field	Description
Total number of BGP4 routes (NLRIs) Installed	Number of BGP4 routes the device has installed in the BGP4 route table.
Distinct BGP4 destination networks	Number of destination networks the installed routes represent. The BGP4 route table can have multiple routes to the same network.
Filtered BGP4 routes for soft reconfig	Number of route updates received from soft-reconfigured neighbors or peer groups that have been filtered out but retained.
Routes originated by this device	Number of routes in the BGP4 route table that this device originated.
Routes selected as BEST routes	Number of routes in the BGP4 route table that this device has selected as the best routes to the destinations.
BEST routes not installed in IP forwarding table	Number of BGP4 routes that are the best BGP4 routes to their destinations but were not installed in the IP route table because the device received better routes from other sources (such as OSPF, RIP, or static IP routes).
Unreachable routes (no IGP route for NEXTHOP)	Number of routes in the BGP4 route table whose destinations are unreachable because the next-hop is unreachable.
IBGP routes selected as best routes	Number of "best" routes in the BGP4 route table that are IBGP routes.
EBGP routes selected as best routes	Number of "best" routes in the BGP4 route table that are EBGP routes.

Examples

The following example shows sample output from the **show ip bgp routes** command.

```
device> show ip bgp routes

Total number of BGP Routes: 2000
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix            Next Hop        MED        LocPrf     Weight Status
1      150.150.150.0/24   103.103.1.1     2          100        0      BEx
         AS_PATH: 201
2      150.150.150.0/24   103.103.2.1     3          100        0      E
         AS_PATH: 202
3      150.150.150.0/24   103.103.3.1     4          100        0      E
         AS_PATH: 203
4      150.150.150.0/24   103.103.4.1     5          100        0      E
         AS_PATH: 204
5      150.150.150.0/24   103.103.5.1     6          100        0      E
…
```

The following example shows sample output from the **show ip bgp routes** command when the **detail** keyword is used.

```
device> show ip bgp routes detail

Total number of BGP 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 S:SUPPRESSED
1       Prefix: 10.5.0.0/24,  Status: BME,  Age: 0h28m28s
         NEXT_HOP: 10.1.1.2,  Learned from Peer: 10.1.0.2 (5)
          LOCAL_PREF: 101,  MED: 0,  ORIGIN: igp,  Weight: 10
           AS_PATH: 5
            Adj_RIB_out count: 4,  Admin distance 20
```

The following example shows sample output from the **show ip bgp routes** command when the **summary** keyword is used.

```
device> show ip bgp routes summary

  Total number of BGP routes (NLRIs) Installed     : 20
  Distinct BGP destination networks                : 20
  Filtered BGP routes for soft reconfig            : 100178
  Routes originated by this router                 : 2
  Routes selected as BEST routes                   : 19
  BEST routes not installed in IP forwarding table : 1
  Unreachable routes (no IGP route for NEXTHOP)    : 1
  IBGP routes selected as best routes              : 0
  EBGP routes selected as best routes              : 17
```

The following example shows sample output from the **show ip bgp routes** command when the **unreachable** keyword is used.

```
device> show ip bgp routes unreachable

Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED
       Prefix      Next Hop        Metric     LocPrf     Weight Status
1      10.8.8.0/24  192.168.5.1     0          101        0
         AS_PATH: 65001 4355 1
```

The following example shows sample output from the **show ip bgp routes** command when an IP address is specified.

```
device> show ip bgp route 10.3.4.0

Number of BGP Routes matching display condition : 1
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network       Next Hop      Metric LocPrf Weight Path
*>  10.3.4.0/24   192.168.4.106        100    0      65001 4355 1 1221 ?
       Last update to IP routing table: 0h11m38s, 1 path(s) installed:
         Gateway           Port
         192.168.2.1       2/1
       Route is advertised to 1 peers:
        10.20.20.2(65300)
```

History

Release version	Command history
6.0.0	Command output was modified to include details about BGP additional paths.

show ip bgp summary

Displays summarized information about the status of all BGP connections.

Syntax

show ip bgp summary

Modes

User EXEC mode

Usage Guidelines

If a BGP4 peer is not configured for an address-family, the peer information is not displayed. If a BGP4 peer is configured for an address-family but not negotiated for an address-family after the BGP4 peer is in the established state, the **show ip bgp summary** command output shows (**NoNeg**) at the end of the line for this peer.

Command Output

The **show ip bgp summary** command displays the following information:

This field	Displays
Router ID	The device ID.
Local AS Number	The BGP4 AS number for the device.
Confederation Identifier	The AS number of the confederation in which the device resides.
Confederation Peers	The numbers of the local autonomous systems contained in the confederation. This list matches the confederation peer list you configure on the device.
Maximum Number of Paths Supported for Load Sharing	The maximum number of route paths across which the device can balance traffic to the same destination. The feature is enabled by default but the default number of paths is 1. You can increase the number from 2 through 8 paths.
Number of Neighbors Configured	The number of BGP4 neighbors configured on this device, and currently in established state.
Number of Routes Installed	The number of BGP4 routes in the device BGP4 route table and the route or path memory usage.
Number of Routes Advertising to All Neighbors	The total of the RtSent and RtToSend columns for all neighbors, the total number of unique ribout group entries, and the amount of memory used by these groups.
Number of Attribute Entries Installed	The number of BGP4 route-attribute entries in the device route-attributes table and the amount of memory used by these entries.
Neighbor Address	The IP addresses of the BGP4 neighbors for this device.
AS#	The AS number.
State	The state of device sessions with each neighbor. The states are from this perspective of the device, not the neighbor. State values are

This field	Displays
	based on the BGP4 state machine values described in RFC 1771 and can be one of the following for each device: • IDLE - The BGP4 process is waiting to be started. Usually, enabling BGP4 or establishing a neighbor session starts the BGP4 process. A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • ADMND - The neighbor has been administratively shut down. • CONNECT - BGP4 is waiting for the connection process for the TCP neighbor session to be completed. • ACTIVE - BGP4 is waiting for a TCP connection from the neighbor. **Note** : If the state frequently changes between CONNECT and ACTIVE, there may be a problem with the TCP connection. • OPEN SENT - BGP4 is waiting for an Open message from the neighbor. • OPEN CONFIRM - BGP4 has received an Open message from the neighbor and is now waiting for either a KEEPALIVE or NOTIFICATION message. If the device receives a KEEPALIVE message from the neighbor, the state changes to Established. If the message is a NOTIFICATION, the state changes to Idle. • ESTABLISHED - BGP4 is ready to exchange UPDATE packets with the neighbor. **Operational States:** Additional information regarding the operational states of BGP described above may be added as described in the following: • **(+)** - is displayed if there is more BGP data in the TCP receiver queue. **Note** : If you display information for the neighbor using the **show ip bgp neighbor***ip-addr* command, the TCP receiver queue value will be greater than 0. • **(>)** - indicates that there is more BGP data in the outgoing queue. • **(-)** - indicates that the session has gone down and the software is clearing or removing routes. • **(*)** - indicates that the inbound or outbound policy is being updated for the peer. • (**c)** - indicates that the table entry is clearing. • (**p)** - indicates that the neighbor ribout group membership change is pending or in progress • **(s)** - indicates that the peer has negotiated restart, and the session is in a stale state. • **(r)** - indicates that the peer is restarting the BGP4 connection, through restart. • **(^)** - on the standby MP indicates that the peer is in the ESTABLISHED state and has received restart capability (in the primary MP). • **(<)** - indicates that the device is waiting to receive the "End of RIB" message the peer.
Time	The time that has passed since the state last changed.
Accepted	The number of routes received from the neighbor that this device installed in the BGP4 route table. Usually, this number is lower than

This field	Displays
	the RoutesRcvd number. The difference indicates that this device filtered out some of the routes received in the UPDATE messages.
Filtered	The routes or prefixes that have been filtered out: • If soft reconfiguration is enabled, this field shows how many routes were filtered out (not placed in the BGP4 route table) but retained in memory. • If soft reconfiguration is not enabled, this field shows the number of BGP4 routes that have been filtered out.
Sent	The number of BGP4 routes the device has sent to the neighbor.
ToSend	The number of routes the device has queued to advertise and withdraw to a neighbor.

Examples

This example displays sample output from the **show ip bgp summary** command.

```
device> show ip bgp summary
   BGP4 Summary
  Router ID: 7.7.7.7   Local AS Number: 100
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 1, UP: 1
  Number of Routes Installed: 0
  Number of Routes Advertising to All Neighbors: 0 (0 entries)
  Number of Attribute Entries Installed: 0
  '+': 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
  10.1.1.8          100         ESTAB   0h 9m16s      0           0        0        0
```

History

Release version	Command history
5.9.00	The command was modified. Description codes were added to display output.

show ip bgp vrf neighbors

Displays configuration information and statistics for BGP4 neighbors of the device for a virtual routing and forwarding (VRF) instance.

Syntax

show ip bgp vrf *vrf-name* **neighbors** [*ip-addr*]

show ip bgp vrf *vrf-name* **neighbors last-packet-with-error**

show ip bgp vrf *vrf-name* **neighbors routes-summary**

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **advertised-routes** [**detail**] [*ip address /mask*]

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **flap-statistics**

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **last-packet-with-error** [**decode**]

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **received** [**prefix-filter**]

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **received-routes** [**detail**]

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **rib-out-routes** [**detail**] [*ipv6 address /mask*]

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **routes**

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **routes** { **best** | **not-installed-best** | **unreachable** }

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** }

show ip bgp vrf *vrf-name* **neighbors** *ip-addr* **routes-summary**

Parameters

vrf-name
Specifies the name of a VRF instance.

neighbors
Specifies a neighbor.

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

last-packet-with-error
Displays the last packet with an error.

routes-summary
Displays routes received, routes accepted, number of routes advertised by peer, and so on.

advertised-routes
Specifies the routes that the device has advertised to the neighbor during the current BGP4 session.

detail
Specifies detailed information.

ip address /mask
Specifies an IP address and mask.

flap-statistics
Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

last-packet-with-error
Specifies the last packet with an error.

decode
Decodes the last packet that contained an error from any of a device's neighbors.

received
Specifies Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

prefix-filter
Displays the results for ORFs that are prefix-based.

received-routes
Specifies all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

rib-out-routes
Displays information about the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

routes
Displays a variety of route information received in UPDATE messages from BGP4 neighbors.

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.

routes-summary
Displays all route information received in UPDATE messages from BGP4 neighbors.

Modes

User EXEC mode

show ip bgp vrf routes

Displays statistics for the routes in the BGP4 route table of a device for a virtual routing and forwarding (VRF) instance.

Syntax

show ip bgp vrf *vrf-name* **routes** [**detail**] [*num* | *ip-address/prefix* | **age** *num* | **as-path-access-list** *name* | **as-path-filter** *number* | **best** | **cidr-only** | **community-access-list** *name* | **community-filter** *number* | **community-reg-expression** *expression* | **local** | **neighbor** *ip-addr* | **nexthop** *ip-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**]

Parameters

vrf-name
Specifies the name of a VRF instance.

detail
Displays detailed information.

num
Table entry at which the display starts. For example, if you want to list entries beginning with table entry 100, specify 100.

ip-address/prefix
Specifies an IP address and prefix.

age *num*
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).

as-path-filter *number*
Displays BGP4 route information that is filtered using the specified AS-path filter.

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.

community-filter *number*
Displays BGP4 route information that matches a specific community filter.

community-reg-expression *expression*
Displays BGP4 route information for an ordered community list regular expression.

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 a prefix list.

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.

Modes

User EXEC mode

show ip bgp vrf

Displays entries in the IPv4 Border Gateway Protocol (BGP4) routing table for a virtual routing and forwarding (VRF) instance.

Syntax

show ip bgp vrf *vrf-name*

show ip bgp vrf *vrf-name ipv6 address/ /mask* [**longer-prefixes**]

show ip bgp vrf *vrf-name ip address/* [*/mask*] [**longer-prefixes**]

show ip bgp vrf *vrf-name* **attribute-entries**

show ip bgp vrf *vrf-name* **dampened-paths**

show ip bgp vrf *vrf-name* **filtered-routes** [**detail**] [*ip-addr* { **/** *mask* } [**longer-prefixes**]] | **as-path-access-list** *name*] | **prefix-list** *name*]

show ip bgp vrf *vrf-name* **flap-statistics**

show ip bgp vrf *vrf-name* **flap-statistics** *ip-addr* { **/** *mask* } [**longer-prefix**]

show ip bgp vrf *vrf-name* **flap-statistics as-path-filter** *name*

show ip bgp vrf *vrf-name* **flap-statistics neighbor** *ip-addr*

show ip bgp vrf *vrf-name* **flap-statistics regular-expression** *name*

show ip bgp vrf *vrf-name* **nexthop** [*ip-addr* | **reachable** | **unreachable**]

show ip bgp vrf *vrf-name* **peer-group** *peer-group-name*

show ip bgp vrf *vrf-name* **summary**

Parameters

vrf-name
Specifies the name of a VRF instance.

ipv6 address /mask
Specifies an IPv6 address and mask.

longer-prefixes
Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

ip address /mask
Specifies an IP address and mask.

attribute-entries
Specifies BGP4 route-attribute entries that are stored in device memory.

dampened-paths
Specifies multiprotocol BGP (MBGP) paths that have been dampened by route-flap dampening.

filtered-routes
Specifies BGP4 filtered routes that are received from a neighbor or peer group.

detail
Optionally displays detailed route information.

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.

flap-statistics
Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

as-path-filter *name*
Specifies an AS-path filter.

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.

nexthop
Specifies the configured next hop.

reachable
Specifies reachable next hops.

unreachable
Specifies unreachable next hops.

peer-group *peer-group-name*
Specifies a peer group.

summary
Displays summarized information.

Modes

User EXEC mode

show ip http client

Displays information about the http(s) link and request between the http(s)server and the Brocade device (client).

Syntax

show ip http client

Modes

User EXEC mode.

Usage Guidelines

Command Output

The **show ip http client** command displays the following information:

TABLE 11 Callers

Output field	Description
Session	The session ID
Username	The *username*. (Blank if none used)
Server	The server connection number

TABLE 12 Servers

Output field	Description
Connection	The server connection number
Version	HTTP 1.0 or 1.1
Transport	TCP or TLS
Request	Current request number being processed
IP Address[:Port]	Remote server IPv4 or IPv6 address, and port (if non-default port)

Number	The Request number
Method	GET, PUT, ...

Examples

The following example shows the output from a **show ip http client** command:

```
device# show ip http client
Callers:
Session    Username    Server
1          lab         1

Servers:
Connection Version Transport Request IP Address
1          1.0     TCP       1       10.25.104.10

Requests:
Number Method
1        GET
```

NOTE

There is no history of prior connections being maintained. Once the file transfer is completed, the HTTP(S) session will be closed, and it will no longer be visible under the Server connections.

History

Release	Command History
05.9.00	This command was introduced.

show ip icmp fast-echo-reply

Displays IP Internet Control Message Protocol (ICMP) offload data for the default virtual routing and forwarding (VRF) instance.

Syntax

show ip icmp fast -echo-reply [**detail**]

Parameters

detail

Specifies to display more data from the line cards.

Modes

User EXEC mode

Examples

The **show ip icmp fast-echo-reply** command displays the following information.

```
device# show ip icmp fast-echo-reply
IP ICMP offload data for VRF [default-vrf], Index 0
Total count                  2
Total IPCs 152, Failurs 0 [All VRFs]

Destination           Source               Ageout (Sec)
-------------------------------------------------------
  71.1.1.1             71.1.1.2/8           50
No. of download(s) 30, Fail 0, Asymmetric 0
  10.1.1.3             10.1.1.2/24          50
No. of download(s) 8, Fail 0, Asymmetric 0
```

The following example displays the details of the IP ICMP fast echo reply configuration on the management plane.

```
device# show ip icmp fast-echo-reply detail
Size of ITC/IPC 1828, ICMP data 512
IP ICMP offload data for VRF [default-vrf], VRF Index 0
-------------------------------------------------------
Slot: 5
Number of entries 0
Slot: 7
Number of entries 2
  SRC 71.1.1.2, DST 71.1.1.1, Gateway 71.1.1.2
       InPort 7/12, Tx FID 0x00000053, Counter 519376702, Ageout 50

  SRC 10.1.1.2, DST 10.1.1.3, Gateway 10.1.1.2
       InPort 7/10, Tx FID 0x00000051, Counter 182, Ageout 50
```

The following example displays the details of the IP ICMP fast echo reply configuration on a line card.

```
device# show ip icmp fast-echo-reply
Total packet handled by PBIF        : 523521428
Table full count                    : 0
Total offload handled               : 39
VRF: 0, SRC (host) 71.1.1.2, DST (local) 71.1.1.1, gateway 71.1.1.2, DMAC 0010.9400.00b1
  Ageout 50, counter 523517191, tick 0, Tx FID 0x00000053 (Port 299 (7/12)), In Port 299 (7/12)
  [0x0000cc00: 0x47010102] [0x0000cc04: 0x47010101] [0x0000cc08: 0x012b0047] [0x0000cc0c: 0x10700053]
[0x0000cc10: 0x00100000]
  [0x0000cc14: 0x0053c441] [0x0000cc18: 0x00900047] [0x0000cc1c: 0xffc00110] [0x0000cc20: 0x00000000]
[0x0000cc24: 0x940000b1]

VRF: 0, SRC (host) 10.1.1.2, DST (local) 10.1.1.3, gateway 10.1.1.2, DMAC 0030.48d5.d08b
  Ageout 50, counter 128, tick 0, Tx FID 0x00000051 (Port 297 (7/10)), In Port 297 (7/10)
  [0x0000cc30: 0x0a010102] [0x0000cc34: 0x0a010103] [0x0000cc38: 0x01290001] [0x0000cc3c: 0x10700051]
[0x0000cc40: 0x00300000]
  [0x0000cc44: 0x0051c441] [0x0000cc48: 0x00900001] [0x0000cc4c: 0xffc00204] [0x0000cc50: 0x00000000]
[0x0000cc54: 0x48d5d08b]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cc60: 0x00000000] [0x0000cc64: 0x00000000] [0x0000cc68: 0x00000000] [0x0000cc6c: 0x00000000]
[0x0000cc70: 0x00000000]
  [0x0000cc74: 0x00000000] [0x0000cc78: 0x00000000] [0x0000cc7c: 0x00000000] [0x0000cc80: 0x00000000]
[0x0000cc84: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cc90: 0x00000000] [0x0000cc94: 0x00000000] [0x0000cc98: 0x00000000] [0x0000cc9c: 0x00000000]
[0x0000cca0: 0x00000000]
  [0x0000cca4: 0x00000000] [0x0000cca8: 0x00000000] [0x0000ccac: 0x00000000] [0x0000ccb0: 0x00000000]
[0x0000ccb4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ccc0: 0x00000000] [0x0000ccc4: 0x00000000] [0x0000ccc8: 0x00000000] [0x0000cccc: 0x00000000]
[0x0000ccd0: 0x00000000]
  [0x0000ccd4: 0x00000000] [0x0000ccd8: 0x00000000] [0x0000ccdc: 0x00000000] [0x0000cce0: 0x00000000]
[0x0000cce4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ccf0: 0x00000000] [0x0000ccf4: 0x00000000] [0x0000ccf8: 0x00000000] [0x0000ccfc: 0x00000000]
[0x0000cd00: 0x00000000]
  [0x0000cd04: 0x00000000] [0x0000cd08: 0x00000000] [0x0000cd0c: 0x00000000] [0x0000cd10: 0x00000000]
[0x0000cd14: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cd20: 0x00000000] [0x0000cd24: 0x00000000] [0x0000cd28: 0x00000000] [0x0000cd2c: 0x00000000]
[0x0000cd30: 0x00000000]
  [0x0000cd34: 0x00000000] [0x0000cd38: 0x00000000] [0x0000cd3c: 0x00000000] [0x0000cd40: 0x00000000]
[0x0000cd44: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cd50: 0x00000000] [0x0000cd54: 0x00000000] [0x0000cd58: 0x00000000] [0x0000cd5c: 0x00000000]
[0x0000cd60: 0x00000000]
  [0x0000cd64: 0x00000000] [0x0000cd68: 0x00000000] [0x0000cd6c: 0x00000000] [0x0000cd70: 0x00000000]
[0x0000cd74: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cd80: 0x00000000] [0x0000cd84: 0x00000000] [0x0000cd88: 0x00000000] [0x0000cd8c: 0x00000000]
[0x0000cd90: 0x00000000]
  [0x0000cd94: 0x00000000] [0x0000cd98: 0x00000000] [0x0000cd9c: 0x00000000] [0x0000cda0: 0x00000000]
[0x0000cda4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
```

```
  [0x0000cdb0: 0x00000000] [0x0000cdb4: 0x00000000] [0x0000cdb8: 0x00000000] [0x0000cdbc: 0x00000000]
[0x0000cdc0: 0x00000000]
  [0x0000cdc4: 0x00000000] [0x0000cdc8: 0x00000000] [0x0000cdcc: 0x00000000] [0x0000cdd0: 0x00000000]
[0x0000cdd4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cde0: 0x00000000] [0x0000cde4: 0x00000000] [0x0000cde8: 0x00000000] [0x0000cdec: 0x00000000]
[0x0000cdf0: 0x00000000]
  [0x0000cdf4: 0x00000000] [0x0000cdf8: 0x00000000] [0x0000cdfc: 0x00000000] [0x0000ce00: 0x00000000]
[0x0000ce04: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ce10: 0x00000000] [0x0000ce14: 0x00000000] [0x0000ce18: 0x00000000] [0x0000ce1c: 0x00000000]
[0x0000ce20: 0x00000000]
  [0x0000ce24: 0x00000000] [0x0000ce28: 0x00000000] [0x0000ce2c: 0x00000000] [0x0000ce30: 0x00000000]
[0x0000ce34: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ce40: 0x00000000] [0x0000ce44: 0x00000000] [0x0000ce48: 0x00000000] [0x0000ce4c: 0x00000000]
[0x0000ce50: 0x00000000]
  [0x0000ce54: 0x00000000] [0x0000ce58: 0x00000000] [0x0000ce5c: 0x00000000] [0x0000ce60: 0x00000000]
[0x0000ce64: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ce70: 0x00000000] [0x0000ce74: 0x00000000] [0x0000ce78: 0x00000000] [0x0000ce7c: 0x00000000]
[0x0000ce80: 0x00000000]
  [0x0000ce84: 0x00000000] [0x0000ce88: 0x00000000] [0x0000ce8c: 0x00000000] [0x0000ce90: 0x00000000]
[0x0000ce94: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cea0: 0x00000000] [0x0000cea4: 0x00000000] [0x0000cea8: 0x00000000] [0x0000ceac: 0x00000000]
[0x0000ceb0: 0x00000000]
  [0x0000ceb4: 0x00000000] [0x0000ceb8: 0x00000000] [0x0000cebc: 0x00000000] [0x0000cec0: 0x00000000]
[0x0000cec4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ced0: 0x00000000] [0x0000ced4: 0x00000000] [0x0000ced8: 0x00000000] [0x0000cedc: 0x00000000]
[0x0000cee0: 0x00000000]
  [0x0000cee4: 0x00000000] [0x0000cee8: 0x00000000] [0x0000ceec: 0x00000000] [0x0000cef0: 0x00000000]
[0x0000cef4: 0x00000000]

[Debug registers dumped]
icmp_checksum_err_count (0x0000cf50): Value 0x00000000
Rx Debug data (0x0000cf54): Value 0x00000000
Rx Debug data (0x0000cf58): Value 0x00000000
Rx Debug data (0x0000cf5c): Value 0x00000000
Partial packet dump (0x0000cf60 ~ 0x0000cf8c)
[0x00900693] [0x000005f0] [0x08009c50] [0x00474aea]
[0xeec00000] [0x00000024] [0x3887ed00] [0x00112222]
[0x33440800] [0x10a0b178] [0x00000000] [0x00000000]
```

History

Release version	Command history
5.7.00	This command was introduced.

show ip icmp vrf fast-echo-reply

Displays IP Internet Control Message Protocol (ICMP) offload data for the non-default virtual routing and forwarding (VRF) instance.

Syntax

show ip icmp vrf *vrf-name* **fast -echo-reply** [**detail**]

Parameters

vrf *vrf-name*

Displays VRF ICMP data for a specific VRF instance.

detail

Specifies to display more data from the line cards.

Modes

User EXEC mode

Usage Guidelines

The **vrf** *vrf-name* parameter is supported only on a management module.

Examples

The **show ip icmp vrf fast-echo-reply** command displays the following information on the management plane .

```
device# show ip icmp vrf ping_test fast-echo-reply
IP ICMP offload data for VRF [ping_test], Index 1
Total count                  1
Total IPCs 154, Failurs 0 [All VRFs]

Destination           Source               Ageout (Sec)
-------------------------------------------------------
  10.1.1.3             10.1.1.2/24          60
No. of download(s) 1, Fail 0, Asymmetric 0
```

The following example displays the details of the IP ICMP fast echo reply configuration on the MP.

```
device# show ip icmp vrf TEST fast-echo-reply detail
Size of ITC/IPC 1828, ICMP data 512
IP ICMP offload data for VRF [ping_test], VRF Index 1
-------------------------------------------------------
Slot: 5
Number of entries 0
Slot: 7
Number of entries 1
  SRC 10.1.1.2, DST 10.1.1.3, Gateway 10.1.1.2
       InPort 7/10, Tx FID 0x00000051, Counter 16, Ageout 60
```

The following example displays the details of the IP ICMP fast echo reply configuration on the line card .

```
device# show ip icmp vrf TEST fast-echo-reply detail
Total packet handled by PBIF        : 527321511
Table full count                    : 0
Total offload handled               : 40
VRF: 0, SRC (host) 71.1.1.2, DST (local) 71.1.1.1, gateway 71.1.1.2, DMAC 0010.9400.00b1
  Ageout 50, counter 527316898, tick 0, Tx FID 0x00000053 (Port 299 (7/12)), In Port 299 (7/12)
  [0x0000cc00: 0x47010102] [0x0000cc04: 0x47010101] [0x0000cc08: 0x012b0047] [0x0000cc0c: 0x10700053]
[0x0000cc10: 0x00100000]
  [0x0000cc14: 0x0053c441] [0x0000cc18: 0x00900047] [0x0000cc1c: 0xffc00110] [0x0000cc20: 0x00000000]
[0x0000cc24: 0x940000b1]

VRF: 1, SRC (host) 10.1.1.2, DST (local) 10.1.1.3, gateway 10.1.1.2, DMAC 0030.48d5.d08b
  Ageout 60, counter 54, tick 0, Tx FID 0x00000051 (Port 297 (7/10)), In Port 297 (7/10)
  [0x0000cc30: 0x0a010102] [0x0000cc34: 0x0a010103] [0x0000cc38: 0x01290001] [0x0000cc3c: 0x10700051]
[0x0000cc40: 0x00300000]
  [0x0000cc44: 0x0051c441] [0x0000cc48: 0x00900001] [0x0000cc4c: 0xffc00204] [0x0000cc50: 0x00000001]
[0x0000cc54: 0x48d5d08b]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cc60: 0x00000000] [0x0000cc64: 0x00000000] [0x0000cc68: 0x00000000] [0x0000cc6c: 0x00000000]
[0x0000cc70: 0x00000000]
  [0x0000cc74: 0x00000000] [0x0000cc78: 0x00000000] [0x0000cc7c: 0x00000000] [0x0000cc80: 0x00000000]
[0x0000cc84: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cc90: 0x00000000] [0x0000cc94: 0x00000000] [0x0000cc98: 0x00000000] [0x0000cc9c: 0x00000000]
[0x0000cca0: 0x00000000]
  [0x0000cca4: 0x00000000] [0x0000cca8: 0x00000000] [0x0000ccac: 0x00000000] [0x0000ccb0: 0x00000000]
[0x0000ccb4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ccc0: 0x00000000] [0x0000ccc4: 0x00000000] [0x0000ccc8: 0x00000000] [0x0000cccc: 0x00000000]
[0x0000ccd0: 0x00000000]
  [0x0000ccd4: 0x00000000] [0x0000ccd8: 0x00000000] [0x0000ccdc: 0x00000000] [0x0000cce0: 0x00000000]
[0x0000cce4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ccf0: 0x00000000] [0x0000ccf4: 0x00000000] [0x0000ccf8: 0x00000000] [0x0000ccfc: 0x00000000]
[0x0000cd00: 0x00000000]
  [0x0000cd04: 0x00000000] [0x0000cd08: 0x00000000] [0x0000cd0c: 0x00000000] [0x0000cd10: 0x00000000]
[0x0000cd14: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cd20: 0x00000000] [0x0000cd24: 0x00000000] [0x0000cd28: 0x00000000] [0x0000cd2c: 0x00000000]
[0x0000cd30: 0x00000000]
  [0x0000cd34: 0x00000000] [0x0000cd38: 0x00000000] [0x0000cd3c: 0x00000000] [0x0000cd40: 0x00000000]
[0x0000cd44: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cd50: 0x00000000] [0x0000cd54: 0x00000000] [0x0000cd58: 0x00000000] [0x0000cd5c: 0x00000000]
```

```
[0x0000cd60: 0x00000000]
  [0x0000cd64: 0x00000000] [0x0000cd68: 0x00000000] [0x0000cd6c: 0x00000000] [0x0000cd70: 0x00000000]
[0x0000cd74: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cd80: 0x00000000] [0x0000cd84: 0x00000000] [0x0000cd88: 0x00000000] [0x0000cd8c: 0x00000000]
[0x0000cd90: 0x00000000]
  [0x0000cd94: 0x00000000] [0x0000cd98: 0x00000000] [0x0000cd9c: 0x00000000] [0x0000cda0: 0x00000000]
[0x0000cda4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cdb0: 0x00000000] [0x0000cdb4: 0x00000000] [0x0000cdb8: 0x00000000] [0x0000cdbc: 0x00000000]
[0x0000cdc0: 0x00000000]
  [0x0000cdc4: 0x00000000] [0x0000cdc8: 0x00000000] [0x0000cdcc: 0x00000000] [0x0000cdd0: 0x00000000]
[0x0000cdd4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cde0: 0x00000000] [0x0000cde4: 0x00000000] [0x0000cde8: 0x00000000] [0x0000cdec: 0x00000000]
[0x0000cdf0: 0x00000000]
  [0x0000cdf4: 0x00000000] [0x0000cdf8: 0x00000000] [0x0000cdfc: 0x00000000] [0x0000ce00: 0x00000000]
[0x0000ce04: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ce10: 0x00000000] [0x0000ce14: 0x00000000] [0x0000ce18: 0x00000000] [0x0000ce1c: 0x00000000]
[0x0000ce20: 0x00000000]
  [0x0000ce24: 0x00000000] [0x0000ce28: 0x00000000] [0x0000ce2c: 0x00000000] [0x0000ce30: 0x00000000]
[0x0000ce34: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ce40: 0x00000000] [0x0000ce44: 0x00000000] [0x0000ce48: 0x00000000] [0x0000ce4c: 0x00000000]
[0x0000ce50: 0x00000000]
  [0x0000ce54: 0x00000000] [0x0000ce58: 0x00000000] [0x0000ce5c: 0x00000000] [0x0000ce60: 0x00000000]
[0x0000ce64: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ce70: 0x00000000] [0x0000ce74: 0x00000000] [0x0000ce78: 0x00000000] [0x0000ce7c: 0x00000000]
[0x0000ce80: 0x00000000]
  [0x0000ce84: 0x00000000] [0x0000ce88: 0x00000000] [0x0000ce8c: 0x00000000] [0x0000ce90: 0x00000000]
[0x0000ce94: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000cea0: 0x00000000] [0x0000cea4: 0x00000000] [0x0000cea8: 0x00000000] [0x0000ceac: 0x00000000]
[0x0000ceb0: 0x00000000]
  [0x0000ceb4: 0x00000000] [0x0000ceb8: 0x00000000] [0x0000cebc: 0x00000000] [0x0000cec0: 0x00000000]
[0x0000cec4: 0x00000000]

VRF: 0, SRC (host) 0.0.0.0, DST (local) 0.0.0.0, gateway 0.0.0.0, DMAC 0000.0000.0000
  Entry not active.
  [0x0000ced0: 0x00000000] [0x0000ced4: 0x00000000] [0x0000ced8: 0x00000000] [0x0000cedc: 0x00000000]
[0x0000cee0: 0x00000000]
  [0x0000cee4: 0x00000000] [0x0000cee8: 0x00000000] [0x0000ceec: 0x00000000] [0x0000cef0: 0x00000000]
[0x0000cef4: 0x00000000]

[Debug registers dumped]
icmp_checksum_err_count (0x0000cf50): Value 0x00000000
Rx Debug data (0x0000cf54): Value 0x00000000
Rx Debug data (0x0000cf58): Value 0x00000000
Rx Debug data (0x0000cf5c): Value 0x00000000
Partial packet dump (0x0000cf60 ~ 0x0000cf8c)
[0x00900693] [0x000005f0] [0x08009c50] [0x00474aea]
[0xeec00000] [0x00000024] [0x3887ed00] [0x00112222]
[0x33440800] [0x1fb386d8] [0x00000000] [0x00000000]
```

History

Release version	Command history
5.7.00	This command was introduced.

show ip igmp cluster-client

Displays the IGMP cluster groups.

Syntax

show ip igmp cluster-client [**group** *group-address* [**detail**]]

Parameters

group *group-address*

Specifies the IGMP multicast-group IP address in dotted-decimal notation.

detail

Displays detailed information.

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays all IGMP cluster groups.

```
device# show ip igmp cluster-client
Total 1 groups
--------------------------------------------------------------------------------
Idx   Group Address    Port   Intf   GrpCmpV Mode    Timer Refreshed MDUPReq Srcs
----+---------------+------+------+-------+-------+------+---------+-------+------
   1  10.1.1.1        e1/7   v10       Ver2 exclude   237      N        N     0
```

History

Release version	Command history
06.1.00	This command was introduced.

show ip igmp group count

Displays the total number of IGMP groups.

Syntax

show ip igmp group count

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays the total number of IGMP groups.

```
device# show ip igmp group count
Total IGMP groups : 4096
```

History

Release version	Command history
06.1.00	This command was introduced.

show ip pim counter mct

Displays the IGMP MDUP statistics.

Syntax

show ip pim counter mct

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays the IGMP MDUP statistics.

```
device# show ip pim counter mct
Multicast MCT Statistics for IPv4 (DN):
Messages assembled into the send buffer  : 0
Messages processed out of the recv buffer: 0
Segments sent successfully to TCP        : 0
Segments failed to be accepted by TCP    : 0
Segments assembed into the receive buffer: 0
Messages dropped because (size > 12000)   : 0
Messages dropped because it won't fit into available space in send buffer   : 0
Segments dropped because it won't fit into available space in receive buffer: 0
Received messages dropped because of cluster-id mismatch                    : 0
Received messages dropped because the peer was not recognized               : 0
Received messages dropped because cluster not active                        : 0
Received messages dropped because MCT VLAN unrecognized                     : 0
Received messages dropped because of bad message type                       : 0
Received messages dropped because of bad checksum                           : 0
Received bytes skipped because of sync or checksum errors                   : 0
PIM Hello Messages sent  : 0
PIM J/P Messages sent    : 0
PIM Assert Messages sent : 0
PIM Unknown not sent     : 0
PIM Hello Messages received     : 0
PIM J/P Messages received       : 0
PIM Assert Messages received   : 0
PIM Unknown received & dropped : 0
IGMPv1 reports sent  : 0
IGMPv2 reports sent  : 0
IGMPv3 reports sent    : 0
IGMP leaves sent : 0
IGMP queries sent : 0
IGMP unknown not sent     : 0
IGMPv1 reports received : 0
IGMPv2 reports received : 0
IGMPv3 reports received : 0
IGMP leaves received   : 0
IGMP queries received   : 0
IGMP unknown received & dropped : 0
```

History

Release version	Command history
06.1.00	This command was modified to add MDUP statistics for IGMP packets.

show ip pim global

Displays the global IPv4 PIM settings.

Syntax

show ip pim global

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays the global IPv4 PIM settings.

```
device# show ip pim global
Global IPv4 PIM Settings
  Fast Convergence          : disabled
  Scaling Optimization      : disabled
  MCT Scaling Optimization  : enabled
  LAG Rebalance             : disabled
  ECMP Type                 : disabled
  NSR Status                : disabled
  Trunk OIF Optimization    : enabled
  Port OIF Optimization     : enabled
  Rate-limit pkt cpu     : 4000        Rate-limit pkt reg         : 1000
  Rate-limit first data  : 2000        Rate-limit reg             : 2000
  Rate-limit wrong intf  : 10000       Rate-limit above threshold : 1000
  Rate-limit ageout      : 60000
  Rate-limit Update KAT  : 1000
  PIM Rate update        : 1
  LP stats traversal time: 0
```

History

Release version	Command history
06.1.00	This command was modified to add the MCT Scaling Optimization setting status.

show ip interface

Displays useful information about the configuration and status of the IP protocol and its services, on all interfaces.

Syntax

show ip interface counters | [**ethernet** *slot/port*] | [**loopback** *num*] | [**pos** *slot/port*] | [**tunnel** *num*]

show ip interface ve *num* [**statistics** [**detail** | **ethernet** *slot/port* | [**vpls vlan** *vlan_id*]]

Parameters

counters
Displays the interface level IP counters.

ethernet *slot/port*
Displays the specified Ethernet interface port.

loopback *num*
Displays the loopback interface number.

pos *slot/port*
Displays the POS interface number.

tunnel *num*
Displays the tunnel interface number.

ve *num*
Displays the Virtual Ethernet interface number.

statistics
Displays the interface level IP counters.

detail
Displays the interface IP extended counters in detail.

ethernet *slot/port*
Displays the interface IP counters for the specified port.

vpls
Displays the VPLS-VE end point IP counters.

vlan *vlan_id*
Displays the specified VPLS-VE end point IP counters.

Modes

EXEC mode

Command Output

The **show ip interface** command displays the following information:

Output field	Description
Interface	The type and the slot and port number of the interface.
IP-Address	The IP address of the interface.
OK?	Whether the IP address is configured on the interface.
Method	Whether the IP address is saved in NVRAM. If you have set the IP address for the interface in the CLI, the Method field is "manual".
Status	The link status of the interface. If the user has disabled the interface with the **disable** command, the entry in the 'Status' field is "administratively DOWN". Otherwise, the entry in the 'Status' field is either UP or DOWN.
Protocol	Whether the interface can provide two-way communication. If the IP address is configured and the link status of the interface is up, the entry in the 'Protocol' field is UP. Otherwise, the entry in the 'Protocol' field is DOWN.
VRF	Whether the VRF is configured or set to default.
Flag	Interface flag: • U- Unnumbered • S- Secondary • US- Unnumbered Secondary • V- V-VE over VPLS • VS- S-VE over VPLS Secondary

Examples

The following example displays the **show ip interface** command modified to display a flag "V" when the interface is a VE over VPLS interface. This enhancement is on the MP as well as the LP.

```
device# show ip int
Flags : U-Unnumbered, S-Secondary, US-Unnumbered Secondary, V-VE over VPLS, VS-VE over VPLS Secondary
Interface    IP-Address      OK?  Method  Status  Protocol  VRF           FLAG
mgmt 1       10.25.106.36    YES  NVRAM   up      up        default-vrf
ve 40        10.40.40.1      YES  NVRAM   down    down      default-vrf
ve 150       10.15.15.1      YES  NVRAM   up      up        default-vrf   V
ve 150       10.20.20.1      YES  NVRAM   up      up        default-vrf   V
ve 150       10.15.15.2      YES  NVRAM   up      up        default-vrf   VS
loopback 1   10.1.1.1        YES  NVRAM   up      up        default-vrf
```

The following example displays the **show ip interface ve** *num* command modified to display ve-type information.

```
device# show ip interface ve 77
Interface Ve 77
  type: vpls
  vpls-id: 3 (name: a)
  members: vlan 20 - ethe 2/2, vlan 20 - ethe 2/3, vlan 101 – ethe 4/1, peer – 12.12.2.5
  active: vlan 20 - ethe 2/2, vlan 20 - ethe 2/3, peer – 12.12.2.5
  port disabled
  port state: DOWN
  ip address: 77.77.77.77/24
  Port belongs to VRF: default-vrf
  encapsulation: ETHERNET, mtu: 1500
  directed-broadcast-forwarding: disabled
  ip icmp redirect: enabled
  ip local proxy arp: disabled
  ip ignore gratuitous arp: disabled
  No inbound ip access-list is set
  No outbound ip access-list is set
  No Helper Addresses are configured.
```

The following example displays the **show ip interface tunnel** *num* command modified to display the traffic counters for the IPSec IPv4 tunnel.

```
device#show ip interface tunnel 10
Interface Tunnel 10
  port enabled
  port state: UP
  ip address: 11.11.11.5/24
  Port belongs to VRF: default-vrf
  encapsulation: ETHERNET, mtu: 1431
  directed-broadcast-forwarding: disabled
  ip icmp redirect: enabled
  ip local proxy arp: disabled
  ip ignore gratuitous arp: disabled
  No inbound ip access-list is set
  No outbound ip access-list is set
  No Helper Addresses are configured.
  RxPkts: 100            TxPkts:11200
  RxBytes:150            TxBytes:12544
```

The following example displays the **show ip interface** command with the **ve** *num* **statistics** option. This command is only applicable for G2/G3a modules.

```
device# show ip interface ve 1001 statistics
Extended Routed Counters (only applicable for G2/G3a modules):

VPLS Name: instance1001, VPLS  Id: 1001
Total     RxPkts           TxPkts           RxBytes          TxBytes
          17               0                3478             0


device# show ip interface ve 1001 statistics detail
VPLS Extended Counters (only applicable for G2/G3a modules):
VPLS Name: instance1001, VPLS  Id: 1001
with the
VPLS Vlan: vlan 1001
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 6/6   265              2170             37882            235824
```

The following example displays the **show ip interface** command with the **ve** *num* **statistics detail** option. This command is only applicable for G2/G3a modules.

```
device# show ip interface ve 1001 statistics detail
VPLS Extended Counters (only applicable for G2/G3a modules):
VPLS Name: instance1001, VPLS  Id: 1001

VPLS Vlan: vlan 1001
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 6/6   265              2170             37882            235824
```

The following example displays the **show ip interface** command with the **ve** *num* **statistics vpls vlan** *vlan_id* option. This command is only applicable for G2/G3a modules.

```
device# show ip interface ve 1001 statistics vpls vlan 1001 ethernet 6/6
Extended Routed Counters (only applicable for G2/G3a modules):

VPLS Name: instance1001, VPLS  Id: 1001
Total     RxPkts           TxPkts           RxBytes          TxBytes
          17               0                3478             0
device#
```

History

Release version	Command history
5.4.00	The **show ip interface** command was modified to display a flag "V" if the interface is a VE over VPLS interface. The **show ip interface ve** command was modified to display VPLS-VE specific information. A new 'Type' field is introduced that shows what type of ve interface it is (VLAN or VPLS).This enhancement is only available for the MP.

show ip match-payload-len

Displays details about the current IP payload length system configuration.

Syntax

show ip match-payload-len [**interface ethernet** *slot /port*

Parameters

interface ethernet

Displays resources used for IP multicast snooping.

slot/port

Specifies the interface slot and port.

Modes

User EXEC mode.

Usage Guidelines

Command Output

The **show ip match-payload-len** command displays the following information:

Output field	Description
Slot	Slot number
PPCR	PPCR number
Min-Payload-length	Minimum payload length
Max-Payload-length	Maximum payload length

Examples

This show command displays the configuration for all PPCR on which IP payload length range is configured.

```
device(config)#show ip match-payload-len
IP Match Payload Length Configuration
Slot        PPCR          Min-Payload-length               Max-Payload-length
1             1                   0                               1000
1             2                   700                             1000
2             2                   800                             800
3             1                   700                             1000
3             2                   700                             1000
```

This show command displays the configuration on PPCR of the interface.

```
device(config)#show ip match-payload-len interface ethernet 1/5
IP Match Payload Length Configuration
Slot        PPCR        Min-Payload-length            Max-Payload-length
1             2               0                              1000
```

History

Release version	Command history
6.0.00a	This command was introduced.

show ip pim global

Displays the global IPv4 PIM settings.

Syntax

show ip pim global

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays the global IPv4 PIM settings.

```
device# show ip pim global
Global IPv4 PIM Settings
  Fast Convergence          : disabled
  Scaling Optimization      : disabled
  MCT Scaling Optimization  : enabled
  LAG Rebalance             : disabled
  ECMP Type                 : disabled
  NSR Status                : disabled
  Trunk OIF Optimization    : enabled
  Port OIF Optimization     : enabled
  Rate-limit pkt cpu     : 4000        Rate-limit pkt reg         : 1000
  Rate-limit first data  : 2000        Rate-limit reg             : 2000
  Rate-limit wrong intf  : 10000       Rate-limit above threshold : 1000
  Rate-limit ageout      : 60000
  Rate-limit Update KAT  : 1000
  PIM Rate update        : 1
  LP stats traversal time: 0
```

History

Release version	Command history
06.1.00	This command was modified to add the MCT Scaling Optimization setting status.

show ip mbgp ipv6

Displays IPv6 multicast BGP information.

Syntax

show ip mbgp ipv6 neighbors

show ip mbgp ipv6 neighbors *ip-addr* **advertised-routes** [**detail**] [*ipv6 address /mask*]

show ip mbgp ipv6 neighbors *ip-addr* **flap-statistics**

show ip mbgp ipv6 neighbors *ip-addr* **last-packet-with-error** [**decode**]

show ip mbgp ipv6 neighbors *ip-addr* **received** [**prefix-filter**]

show ip mbgp ipv6 neighbors *ip-addr* **received-routes** [**detail**]

show ip mbgp ipv6 neighbors *ip-addr* **rib-out-routes** [**detail**] [*ipv6 address /mask*]

show ip mbgp ipv6 neighbors *ip-addr* **routes**

show ip mbgp ipv6 neighbors *ip-addr* **routes** { **best** | **not-installed-best** | **unreachable** }

show ip mbgp ipv6 neighbors *ip-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** }

show ip mbgp ipv6 neighbors *ip-addr* **routes-summary**

show ip mbgp ipv6 neighbors last-packet-with-error

show ip mbgp ipv6 neighbors routes-summary

show ip mbgp ipv6 summary

Parameters

neighbors

Specifies a neighbor.

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

advertised-routes

Specifies the routes that the device has advertised to the neighbor during the current BGP4 session.

detail

Specifies detailed information.

ipv6 address /mask

Specifies an IPv6 address and mask.

flap-statistics

Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

last-packet-with-error

Specifies the last packet with an error.

decode

Decodes the last packet that contained an error from any of a device's neighbors.

received
Specifies Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

prefix-filter
Displays the results for ORFs that are prefix-based.

received-routes
Specifies all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

rib-out-routes
Displays information about the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

routes
Displays a variety of route information received in UPDATE messages from BGP4 neighbors.

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.

routes-summary
Displays all route information received in UPDATE messages from BGP4 neighbors.

summary
Displays summarized IPv6 unicast information.

Modes

User EXEC mode

show ip multicast

Displays details about the resources used for IP multicast snooping and IGMP snooping entries on all VLANs.

Syntax

show ip multicast [**resource** | **static** |**vlan***vlan-id* [*A.B.C.D*| **igmpv3** | **pim** | **static** | **statistics** | **tracking**]]

Parameters

resource
Displays resources used for IP multicast snooping.

static
Displays configured static IGMP snooping entries in all VLANs.

vlan *vlan-id*
Specifies the VLAN.

A.B.C.D
Specifies the group address to display IP multicast information.

igmpv3
Displays IGMPv3-specific information.

pim
Displays PIM-specific information.

static
Displays configured IGMP snooping entries.

statistics
Displays IP multicast statistics.

tracking
Displays IGMPv3 host tracking information.

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

You can display IP multicast traffic information in a brief form for all instances or in a detailed form for a specified VLAN or VPLS instance.

Command Output

The **show ip multicast vlan** command displays the following information:

Output field	Description
VLAN	Shows the ID of the configured VLAN.
State	Shows whether the VLAN interface is enabled or disabled.
Mode	Shows whether the VLAN interface is in active mode or passive mode.
Active Querier	Shows the active IGMP querier for the VLAN.
Time Query	Shows the time countdown to generate the next query message.
(*, G) Count	Shows the count of (*,G) entries.
(S, G) Count	Shows the count of (S,G) entries.
Flags	Shows the flags of the outgoing interface.
V2|V3	Shows the version of the IGMP message received.
P_G	Indicates that a PIM (*,G) join was received on that interface.
P_SG	Indicates that a PIM (S,G) join was received on that interface.
NumOIF	Shows the count of the outgoing interface.
profile	Shows the profile ID associated with the stream.
Outgoing Interfaces	Shows the list of outgoing interfaces.
FID	Shows the FID resource allocated for a particular entry.
MVID	Shows the MVID resource allocated for a particular entry.

The **show ip multicast vlan** *vlan-id* **pim**command displays the following information:

Output field	Description
VLAN	Shows the ID of the configured VLAN.
Group	Shows the IP address of the multicast group.
Port	Shows the ports attached to the group's receivers. A port is listed here when it receives a join message for the group, an IGMP membership report for the group, or both.
Join-Source	Shows the IP address from which a join message was received.
age	Shows the join-source age.
Prune-Source	Shows the IP address for pruning a source.
age	Shows the prune-source age.

Examples

The following example displays the IP multicast resources.

```
device# show ip multicast resource
                      allocated(U)    in-use(U) available(U) allo-fail(U)  up-limit(U)
vlanextn                       255           10          245            0         4095
l2mdb                          255            1          254            0         2048
portlist                       255            2          253            0         8192
v3group                        256            0          256            0         8192
v3phyport                     1024            0         1024            0        32768
v3source                      1024            0         1024            0        32768
v3client                      1024            0         1024            0        32768
remote entry                  1024            0         1024            0        32768
HW MVID: 0 allocated for L2MCAST of total allocated 0
```

The following example displays the static entries configured on the VLAN.

```
device# show ip multicast static
Static Entries Configured in VLAN: 2

(*, 230.10.10.10)
Static Uplink: No
Interface Port List: e 2/1
```

The following example displays the static entries configured on VLAN 2.

```
device# show ip multicast vlan 2 static
Static Entries Configured in VLAN: 2

(*, 230.10.10.10)
Static Uplink: No
Interface Port List: e 2/1
```

The following example shows the multicast entries for VLAN 1500.

```
device# show ip multicast vlan 1500
----------+-----+---------+---------------+-----+-----+------
VLAN       State Mode      Active          Time (*, G)(S, G)
                           Querier         Query Count Count
----------+-----+---------+---------------+-----+-----+------
1500       I-Ena Passive   10.25.10.10     103   1     3
----------+-----+---------+---------------+-----+-----+------


Router ports: 7/16 (60s)


Flags-  R: Router Port,  V2|V3: IGMP Receiver,  P_G|P_SG: PIM Join


  1    (*, 239.10.10.10) Uptime: 00:01:38       NumOIF: 1       profile: none
         Outgoing Interfaces:
              e7/16 vlan 1500  00:01:38 Flags: ( R [60s] V2 [72s])


  1    (10.25.120.131, 239.10.10.10) in e4/1 vlan 1500 Uptime: 00:00:06         NumOIF: 1  profile: none
         Outgoing Interfaces:
              e7/16 vlan 1500  00:00:06 Flags: ( R V2)

         FID: 0xa013     MVID: None


  2    (10.25.120.130, 239.10.10.10) in e4/1 vlan 1500 Uptime: 00:00:06         NumOIF: 1  profile: none
         Outgoing Interfaces:
              e7/16 vlan 1500  00:00:06 Flags: ( R V2)

         FID: 0xa012     MVID: None


  3    (10.25.120.129, 239.10.10.10) in e4/1 vlan 1500 Uptime: 00:01:39         NumOIF: 1  profile: none
         Outgoing Interfaces:
              e7/16 vlan 1500  00:01:39 Flags: ( R V2)

         FID: 0xa011     MVID: None
```

The following example displays the PIM SM information for VLAN 2.

```
device(config)# show ip multicast vlan 2 pim
Number of PIM Groups:5
Total Number of PIM Entries: 5
vlan group port join-source age prune-source age
---- --------- ---- ---------- --- ------------ ---
2 229.0.0.5 1/1 2.1.1.100 180
2 229.0.0.4 1/1 2.1.1.100 180
2 229.0.0.3 1/1 2.1.1.100 180
2 229.0.0.2 1/1 2.1.1.100 180
2 229.0.0.1 1/1 2.1.1.100 180
```

The following example displays the IP multicast statistics for VLAN 1.

```
device# show ip multicast vlan 1 statistics
IP multicast is enabled - Passive
VLAN ID 1
Reports Received: 34
Leaves Received: 21
General Queries Received: 60
Group Specific Queries Received: 2
Others Received: 0
General Queries Sent: 0
Group Specific Queries Sent: 0
```

History

Release version	Command history
6.0.00	The output for the **show ip multicast vlan** command was modified to include a separate timer for each flag type in a (*, G) entry.

show ip multicast vpls

Displays details about the multicast VPLS instance.

Syntax

show ip multicast vpls *vpls-ID*

Parameters

vpls-ID

The VPLS ID of the VPLS for which to display the IP multicast PIM information.

Modes

User EXEC mode

Privileged EXEC mode

Command Output

The **show ip multicast vpls** command displays the following information:

Output field	Description
VPLS	Shows the ID of the configured VPLS.
State	Shows whether the VPLS interface is enabled or disabled.
Mode	Shows whether the VPLS interface is in active mode or passive mode.
Active Querier	Shows the active IGMP querier for the VPLS.
Time Query	Shows the time countdown to generate the next query message.
(*, G) Count	Shows the count of (*,G) entries.
(S, G) Count	Shows the count of (S,G) entries.
Router ports	Shows the ports through which the multicast sources can be reached.
VC Label	Shows the MPLS VC label.
R Label	Shows the MPLS remote label.
PIM NBR	Shows the PIM neighbor port.
Flags	Shows the interface flag for the entry.
V2|V3	Shows the version of the IGMP message received.
P_G	Indicates that a PIM (*,G) join was received on that interface.
P_SG	Indicates that a PIM (S,G) join was received on that interface.
Mapped MAC Address	Shows the multicast MAC address corresponding to the group.
NumOIF	Shows the count of the outgoing interface.
Profile	Shows the profile ID associated with the stream.
Outgoing Interfaces	Shows the list of outgoing interfaces.
FID	Shows the FID resource allocated for a particular entry.
Mapped group address	Shows the mapped group address.

Output field	Description
MVID	Shows the MVID resource allocated for a particular entry.
TNNL peer	Shows the MPLS peer address.

Examples

The following example displays detailed IP multicast traffic reduction information for VPLS 1.

```
device# show ip multicast vpls 1
----------+-----+---------+---------------+-----+-----+------
VPLS       State Mode      Active          Time (*, G)(S, G)
                           Querier         Query Count Count
----------+-----+---------+---------------+-----+-----+------
1          Ena   Active    122.122.122.122 7     500   500
----------+-----+---------+---------------+-----+-----+------

Router ports: TNNL peer 122.122.122.122 (2s) VC Label 983040

Flags-  R: Router Port,  V2|V3: IGMP Receiver,  P_G|P_SG: PIM Join

  1    (*, 230.0.0.68) Uptime: 13:04:53         NumOIF: 3       profile: none
         Mapped MAC Address: 0100.5e00.0044  FID: 0x0280
         Outgoing Interfaces:
              TNNL peer 124.124.124.124 12:48:19 Flags: ( V2 [4s])
              e1/10 vlan 200  13:04:45 Flags: ( V3 [2s])
              TNNL peer 122.122.122.122 13:04:53 Flags: ( R [2s] V3 [10s])

  1    (200.1.1.100, 230.0.0.68) in e1/11 vlan 200 Uptime: 13:04:53     NumOIF: 3  profile: none
         Outgoing Interfaces:
              TNNL peer 124.124.124.124 VC Label 983040 Port e1/5 12:48:19 Flags: ( V2)
              e1/10 vlan 200  13:04:45 Flags: ( V3)
              TNNL peer 122.122.122.122 VC Label 983040 Port e1/20 13:04:53 Flags: ( R V3)
         FID: 0x0473     MVID:      0
```

The following example displays detailed information about the VPLS instance for IGMPv3.

```
device# show ip multicast vpls 1 igmpv3
vlan in-vlan group               port         mode/ag          permit src/age                deny src
---- ------- ------------------- ------------ ------- ------------------------ ------------------------
200  -       230.0.1.243         1/10         INC             200.1.1.100/205
-    -       230.0.1.243         peer 124.124 INC             200.1.1.100/200
200  -       230.0.1.242         1/10         INC             200.1.1.100/205
-    -       230.0.1.242         peer 124.124 INC             200.1.1.100/200
200  -       230.0.1.241         1/10         INC             200.1.1.100/205
-    -       230.0.1.241         peer 124.124 INC             200.1.1.100/200
200  -       230.0.1.240         1/10         INC             200.1.1.100/205
-    -       230.0.1.240         peer 124.124 INC             200.1.1.100/200
200  -       230.0.1.239         1/10         INC             200.1.1.100/205
-    -       230.0.1.239         peer 124.124 INC             200.1.1.100/200
200  -       230.0.0.0           1/10         INC             200.1.1.100/200
-    -       230.0.0.0           peer 124.124 INC             200.1.1.100/200
```

The following example displays statistics for VPLS 1.

```
MLXe8#show ip multicast vpls 1 statistics
VPLS ID 1
  Receive stats:                          Transmit stats:
  General query           : 0             General query           : 8065
  Group specific query    : 0             Group specific query    : 9
  IGMP Report             : 15972         IGMP V2 Proxy Sent      : 0
  IGMP Leave              : 3             IGMP V3 Proxy Sent      : 0
  IGMPV3 Report           : 8005          PIM Proxy Sent          : 0
  IGMPV3 Error            : 0             MCT MDUP msg sent       : 0
  PIMV2 hello             : 0
  PIMV2 join/prune        : 0
  PIMV2 J/P pkt error     : 0
  MCT MDUP msg recvd      : 0
  MCT MDUP msg error      : 0
```

The following example displays VPLS 1 tracking information.

```
vlan group                port         mode/age           permit src/age            client IP/age
---- -------------------  ------------ -------- ------------------------ ------------------------
-    230.0.0.0            peer 123.123 INC               200.1.1.100/25            200.1.1.40/25

MLXe8#show ip multicast vpls 1 pim
  Number of PIM Groups: 0
  Total Number of PIM Entries: 0
vlan group           port  join-source         age  prune-source        age
---- --------------- ----- ------------------- ---- ------------------- ----
```

History

Release version	Command history
6.0.00	The output of the command was modified to include a separate timer for each flag type in a (*, G) entry.

show ip ospf

Displays OSPF information.

Syntax

show ip ospf

Modes

User EXEC mode

Examples

This example displays sample output from the **show ip ospf** command.

```
device> show ip ospf

OSPF Version Version 2
Router Id 10.1.1.2
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 00000000
Originate New LSA Counter 9
Rx New LSA Counter 6
External LSA Limit 174762
Database Overflow Interval 0
Database Overflow State : NOT OVERFLOWED
RFC 1583 Compatibility : Enabled
Slow neighbor Flap-Action : Disabled, timer 300
Nonstop Routing: Disabled
Graceful Restart: Disabled, timer 120
Graceful Restart Helper: Enabled
LDP-SYNC: Globally enabled, Hold-down time 66 sec
Interfaces with LDP-SYNC enabled:
eth 1/3 eth 1/4
```

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** [**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* }]

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.

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.

adv-router *router-id*

Displays the link state for the advertising router 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.

Modes

User EXEC mode

Command Output

The **show ip ospf area** command displays the following information:

Output field	Description
Index	The row number of the entry in the router's OSPF area table.
Area	The area number.
Type	The area type, which can be one of the following: • nssa • normal • stub
Cost	The area's cost.
SPFR	The SPFR value.
ABR	The ABR number.
ASBR	The ABSR number.
LSA	The LSA number.
Chksum(Hex)	The checksum for the LSA packet. The checksum is based on all the fields in the packet except the age field. The device uses the checksum to verify that the packet is not corrupted.

Examples

The following example shows output for the **show ip ospf area** command.

```
device> show ip ospf area

Indx  Area       Type   Cost  SPFR  ABR  ASBR  LSA  Chksum(Hex)
1    0.0.0.0     normal  0    1      0     0    1    0000781f
2  10.147.60.0   normal  0    1      0     0    1    0000fee6
3  10.147.80.0   stub    1    1      0     0    2    000181cd
```

show ip ospf border-routers

Displays information about border routers and boundary routers.

Syntax

show ip ospf border-routers [*A.B.C.D*]

Parameters

A.B.C.D

Specifies the router ID in dotted decimal format.

Modes

User EXEC mode

Usage Guidelines

Use this command to display information about area border routers (ABRs) and autonomous system boundary routers (ASBRs). You can display information for all ABRs and ASBRs or for a specific router.

Command Output

The **show ip ospf border-routers** command displays the following information:

Output field	Description
(Index)	Displayed index number of the border router.
Router ID	ID of the OSPF router
Router type	Type of OSPF router: ABR or ASBR
Next hop router	ID of the next hop router
Outgoing interface	ID of the interface on the router for the outgoing route.
Area	ID of the OSPF area to which the OSPF router belongs

Examples

The following is sample output for the **show ip ospf border-routers** command when no router ID is specified.

```
device> show ip ospf border-routers
      router ID       router type next hop router  outgoing interface  Area
1     10.65.12.1      ABR         10.1.49.2        v49                 0
1     10.65.12.1      ASBR        10.1.49.2        v49                 0
1     10.65.12.1      ABR         10.65.2.251      v201                65
1     10.65.12.1      ASBR        10.65.2.251      v201                65
```

show ip ospf config

Displays general OSPF configuration information.

Syntax

show ip ospf config

Modes

User EXEC mode

Command Output

The **show ip ospf config** command displays the following information:

Output field	Description
Router OSPF	Shows whether or not the router OSPF is enabled.
Nonstop Routing	Shows whether or not the non-stop routing is enabled.
Graceful Restart	Shows whether or not the graceful restart is enabled.
Graceful Restart Helper	Shows whether or not the OSPF graceful restart helper mode is enabled.
Graceful Restart Time	Shows the maximum restart wait time advertised to neighbors.
Graceful Restart Notify Time	Shows the graceful restart notification time.
Redistribution	Shows whether or not the redistribution is enabled.
Default OSPF Metric	Shows the default OSPF metric value.
OSPF Auto-cost Reference Bandwidth	Shows whether or not the auto-cost reference bandwidth option is enabled.
Default Passive Interface	Shows whether or not the default passive interface state is enabled.
OSPF Redistribution Metric	Shows the OSPF redistribution metric type, which can be one of the following: • Type1 • Type2
OSPF External LSA Limit	Shows the external LSA limit value.
OSPF Database Overflow Interval	Shows the database overflow interval value.
RFC 1583 Compatibility	Shows whether or not the RFC 1583 compatibility is enabled.
Router id	Shows the ID of the OSPF router.
OSPF traps	Shows whether or not the following OSPF traps generation is enabled. • Interface State Change Trap • Virtual Interface State Change Trap • Neighbor State Change Trap • Virtual Neighbor State Change Trap • Interface Configuration Error Trap • Virtual Interface Configuration Error Trap • Interface Authentication Failure Trap

Output field	Description
	• Virtual Interface Authentication Failure Trap • Interface Receive Bad Packet Trap • Virtual Interface Receive Bad Packet Trap • Interface Retransmit Packet Trap • Virtual Interface Retransmit Packet Trap • Originate LSA Trap • Originate MaxAge LSA Trap • Link State Database Overflow Trap • Link State Database Approaching Overflow Trap
Area-ID	Shows the area ID of the interface.
Area-Type	Shows the area type, which can be one of the following: • nssa • normal • stub
Cost	Shows the cost of the area.
Ethernet Interface	Shows the OSPF interface.
ip ospf md5-authentication-key-activation-wait-time	Shows the wait time of the device until placing a new MD5 key into effect.
ip ospf area	Shows the area of the interface.
ip ospf cost	Shows the overhead required to send a packet across an interface.

Examples

The following example displays general OSPF configuration information.

```
device> show ip ospf config
Router OSPF: Enabled
Nonstop Routing: Disabled
Graceful Restart: Disabled
Graceful Restart Helper: Enabled
Graceful Restart Time: 120
Graceful Restart Notify Time: 0
Redistribution: Disabled
Default OSPF Metric: 50
OSPF Auto-cost Reference Bandwidth: Disabled
Default Passive Interface: Enabled
OSPF Redistribution Metric: Type2
OSPF External LSA Limit: 1447047
OSPF Database Overflow Interval: 0
RFC 1583 Compatibility: Enabled
Router id: 10.95.11.128
Interface State Change Trap:                        Enabled
Virtual Interface State Change Trap:                Enabled
Neighbor State Change Trap:                         Enabled
Virtual Neighbor State Change Trap:                 Enabled
Interface Configuration Error Trap:                 Enabled
Virtual Interface Configuration Error Trap:         Enabled
Interface Authentication Failure Trap:              Enabled
Virtual Interface Authentication Failure Trap:      Enabled
Interface Receive Bad Packet Trap:                  Enabled
Virtual Interface Receive Bad Packet Trap:          Enabled
Interface Retransmit Packet Trap:                   Disabled
Virtual Interface Retransmit Packet Trap:           Disabled
Originate LSA Trap:                                 Disabled
Originate MaxAge LSA Trap:                          Disabled
Link State Database Overflow Trap:                  Disabled
Link State Database Approaching Overflow Trap:      Disabled
OSPF Area currently defined:
Area-ID          Area-Type Cost
0                normal    0
OSPF Interfaces currently defined:
Ethernet Interface: 3/1-3/2
ip ospf md5-authentication-key-activation-wait-time 300
ip ospf cost 0
ip ospf area 0
Ethernet Interface: v1
ip ospf md5-authentication-key-activation-wait-time 300
ip ospf cost 0
ip ospf area 0
```

show ip ospf database

Shows OSPFv2 database information.

Syntax

show ip ospf database

show ip ospf database database-summary

show ip ospf database external-link-state [**advertise** *index* | **extensive** | **link-state-id** *id* | **router-id** *router-id* | **sequence-number** *num*]

show ip ospf database grace-link-state

show ip ospf database link-state [**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* } | **router-id** *router-id* | **self-originate** | **sequence-number** *num* | **summary** { *id* | **adv-router** *router-id* }]

Parameters

database-summary

Displays how many link state advertisements (LSAs) of each type exist for each area, as well as total number of LSAs.

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

User EXEC mode

Command Output

The **show ip ospf database** command displays the following information:

Output field	Description
Area	The OSPF area that the interface configured for OSPF graceful restart is in.
Interface	The interface that is configured for OSPF graceful restart.
Prd	Grace Period: The number of seconds that the router's neighbors should continue to advertise the router as fully adjacent, regardless of the state of database synchronization between the router and its neighbors. Since this time period began when grace-LSA's LS age was equal to 0, the grace period terminates when either: • the LS age of the grace-LSA exceeds the value of a Grace Period • the grace-LSA is flushed

Output field	Description
Rsn	Graceful restart reason: The reason for the router restart defined as one of the following: • UK – unknown • RS – software restart • UP – software upgrade or reload • SW – switch to redundant control processor
Nbr Intf IP	The IP address of the OSPF graceful restart neighbor.
Index	ID of the entry.
Aging	The age of the LSA in seconds.
Area ID	ID of the OSPF area.
Type	Link state type of the route.
LS ID	The ID of the link-state advertisement from which the router learned this route
Adv Rtr	ID of the advertised route.
Seq (Hex)	The sequence number of the LSA. The OSPF neighbor that sent the LSA stamps the LSA with a sequence number. This number enables the device and other OSPF routers to determine which LSA for a given route is the most recent.
Age	The age of the LSA in seconds.
Chksum	The checksum for the LSA packet. The checksum is based on all the fields in the packet except the age field. The device uses the checksum to verify that the packet is not corrupted.
Router	The router IP address.
Netmask	The subnet mask of the network.
Metric	The cost (value) of the route.
Flag	State information for the route entry. This information is used by Brocade technical support.

Examples

The following example shows output for the **show ip ospf database** command.

```
device> show ip ospf database

Graceful Link States
Area  Interface  Adv Rtr  Age Seq(Hex) Prd Rsn  Nbr Intf IP
0     eth 1/2 10.2.2.2  7   80000001 60  SW 10.1.1.2

Router Link States
Index AreaID            Type LS ID      Adv Rtr     Seq(Hex)   Age  Cksum
1     0                 Rtr 10.2.2.2    10.2.2.2     80000003   93   0xac6c
2     0                 Rtr 10.1.1.1    10.1.1.1     80000005   92   0x699e
3     0                 Net  10.1.1.2   10.2.2.2     80000002   93   0xbd73
4     0                 OpAr 10.0.0.3   10.1.1.1     80000005   83   0x48e7
5     0                 OpAr 10.0.0.2   10.2.2.2     80000006   80   0x50da
6     10.111.111.111    Rtr  10.1.1.1   10.1.1.1     80000004   142  0x0a38
7     10.111.111.111    Summ 10.1.1.1   10.1.1.1     80000001   147  0x292b
8     10.111.111.111    OpAr 10.0.0.2   10.1.1.1     80000002   179  0x063f

Type-5 AS External Link States
Index Age  LS ID     Router   Netmask   Metric    Flag  Fwd Address
1     147 10.9.1.13  10.1.1.1  ffffffff  0000000a  0000  0.0.0.0
2     147 10.9.1.26  10.1.1.1  ffffffff  0000000a  0000  0.0.0.0
```

The following example shows output for the **show ip ospf database** command when the **link-state extensive** parameter is used.

```
device> show ip ospf database link-state extensive

Router LSA:
Area ID         Type LS ID           Adv Rtr         Seq(Hex) Age  Cksum  SyncState
0               Rtr  21.21.21.21     21.21.21.21     80000006 338  0xcd13 Done
  LSA Header: options: -------E-, seq-nbr: 0x80000006, length: 60, flags:-----EB
  link id = 31.31.31.31, link data = 106.50.50.10, type = virtual(4)
  tos count = 0, tos0_metric = 1
  link id = 106.10.10.10, link data = 106.10.10.10, type = transit(2)
  tos count = 0, tos0_metric = 1
  link id = 106.20.20.10, link data = 106.20.20.10, type = transit(2)
  tos count = 0, tos0_metric = 1

Network LSA:
Area ID         Type LS ID           Adv Rtr         Seq(Hex) Age  Cksum  SyncState
0               Net  106.20.20.10    21.21.21.21     80000002 353  0x6285 Done
  LSA Header:  options: -------E-, seq-nbr: 0x80000002, length: 32
  NetworkMask: 255.255.255.0
  attached router: 21.21.21.21
  attached router: 11.11.11.11

NSSA LSA:
Area ID         Type LS ID           Adv Rtr         Seq(Hex) Age  Cksum  SyncState
2               NSSA 2.0.0.0         130.130.130.3   80000001 426  0x780b Done
  LSA Header:  age: 426, options: -----P---, seq-nbr: 0x80000001, length: 36
  NetworkMask: 255.255.255.0
  TOS 0:  metric_type: 2, metric: 10
          forwarding_address: 106.30.30.10
          external_route_tag: 0
```

The following example shows output for the **show ip ospf database** command when the **external-link-state extensive** parameter is used.

```
device> ospf database external-link-state extensive

AS-external LSA
Index Age  LS ID           Router          Netmask  Metric   Flag Fwd Address   SyncState
1     1064 5.1.1.0         21.21.21.21     ffffff00 0000000a 0000 0.0.0.0        Done
  LSA Header:  age: 1064, options: -------E-, seq-nbr: 0x80000001, length: 36
  NetworkMask: 255.255.255.0
  TOS 0:  metric_type: 2, metric: 10
          forwarding_address: 0.0.0.0
          external_route_tag: 0
```

The following example shows output for the **show ip ospf database** command when the **database-summary** parameter is used.

```
device> show ip ospf database database-summary

Area ID    Router Network Sum-Net Sum-ASBR NSSA-Ext Opq-Area Subtotal
0.0.0.0    104    184     19      42       0        0        349
AS External                                                  308
Total      104    184     19      42       0        0        657
```

show ip ospf interface

Displays information about all or specific OSPF-enabled interfaces.

Syntax

show ip ospf interface [*A.B.C.D* | **brief**]

show ip ospf interface [**ethernet** *slot/port* | **loopback** *number* **tunnel** *number* | **ve** *vlan_id*] [**brief**] [**vrf** *vrf-name*]

Parameters

A.B.C.D
Specifies interface IP address in dotted decimal format.

brief
Displays summary information.

ethernet *slot/port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback port number. .

tunnel *number*
Specifies a tunnel interface.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

Modes

User EXEC mode

Command Output

The **show ip ospf interface** command displays the following information:

Output field	Description
Interface	The type of interface type and the port number or number of the interface.
IP Address	The IP address of the interface.
Area	The OSPF area configured on the interface
Database Filter	The router's configuration for blocking outbound LSAs on an OSPF interface. If Not Configured is displayed, there is no outbound LSA filter configured. This is the default condition.
State	The state of the interface. Possible states include the following: • DR - The interface is functioning as the Designated Router for OSPFv2.

Output field	Description
	• BDR - The interface is functioning as the Backup Designated Router for OSPFv2. • Loopback - The interface is functioning as a loopback interface. • P2P - The interface is functioning as a point-to-point interface. • Passive - The interface is up but it does not take part in forming an adjacency. • Waiting - The interface is trying to determine the identity of the BDR for the network. • None - The interface does not take part in the OSPF interface state machine. • Down - The interface is unusable. No protocol traffic can be sent or received on such a interface. • DR other - The interface is a broadcast or NBMA network on which another router is selected to be the DR. • Active - The interface sends or receives all the OSPFv2 control packets and forms the adjacency.
default	Shows whether or not the default passive state is set.
Pri	The interface priority.
Cost	The configured output cost for the interface.
Options	OSPF Options (Bit7 - Bit0): • unused:1 • opaque:1 • summary:1 • dont_propagate:1 • nssa:1 • multicast:1 • external route capable:1 • tos:1
Type	The area type, which can be one of the following: • Broadcast • Point to Point • non-broadcast • Virtual Link
Events	OSPF Interface Event: • Interface_Up = 0x00 • Wait_Timer = 0x01 • Backup_Seen = 0x02 • Neighbor_Change = 0x03 • Loop_Indication = 0x04 • Unloop_Indication = 0x05 • Interface_Down = 0x06 • Interface_Passive = 0x07
Timer intervals	The interval, in seconds, of the transmit-interval, retransmit-interval, hello-interval, and dead-interval timers.
DR	The router ID (IPv4 address) of the DR.
BDR	The router ID (IPv4 address) of the BDR.

Output field	Description
Neighbor Count	The number of neighbors to which the interface is connected.
Adjacent Neighbor Count	The number of adjacent neighbor routers.
Neighbor:	The IP address of the neighbor.

The **show ip ospf interface brief** command displays the following information:

Output field	Description
Interface	The interface through which the router is connected to the neighbor.
Area	The OSPF Area that the interface is configured in.
IP Addr/Mask	The IP address and mask of the interface.
Cost	The configured output cost for the interface.
State	The state of the conversation between the router and the neighbor. This field can have one of the following values: • Down - The initial state of a neighbor conversation. This value indicates that there has been no recent information received from the neighbor. • Attempt - This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor. • Init - A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor. (The router itself did not appear in the neighbor's Hello packet.) All neighbors in this state (or higher) are listed in the Hello packets sent from the associated interface. • 2-Way - Communication between the two routers is bidirectional. This is the most advanced state before beginning adjacency establishment. The Designated Router and Backup Designated Router are selected from the set of neighbors in the 2-Way state or greater. • ExStart - The first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. Neighbor conversations in this state or greater are called adjacencies. • Exchange - The router is describing its entire link state database by sending Database Description packets to the neighbor. Each Database Description packet has a DD sequence number, and is explicitly acknowledged. Only one Database Description packet can be outstanding at any time. In this state, Link State Request packets can also be sent asking for the neighbor's more recent advertisements. All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets. • Loading - Link State Request packets are sent to the neighbor asking for the more recent advertisements that have been discovered (but not yet received) in the Exchange state. • Full - The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network link advertisements.

Output field	Description
Nbrs(F/C)	The number of adjacent neighbor routers. The number to the left of the "/" are the neighbor routers that are fully adjacent and the number to the right represents all adjacent neighbor routers.

Examples

The following example displays OSPF information about a specified Ethernet interface.

```
device> show ip ospf interface ethernet 2/1

eth 2/1 admin up, oper down, ospf enabled, state down
     IP Address 1.1.78.8, Area 1
     Database Filter: Not Configured
     State down, Pri 1, Cost 1, Options ------E-, Type broadcast Events 0
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
```

The following example displays summarized OSPF information about all enabled interfaces.

```
device> show ip ospf interface brief

Number of Interfaces is 1
Interface Area IP Addr/Mask Cost State Nbrs(F/C)
eth 1/2    0    10.1.1.2/24   1     down  0/0
```

show ip ospf neighbor

Displays OSPF neighbor information.

Syntax

show ip ospf neighbor [**extensive** | *num* | **router-id** *A.B.C.D*]

Parameters

extensive

Displays detailed neighbor information.

num

Specifies displays only the entry in the specified index position in the neighbor table. For example, if you enter "1", only the first entry in the table is displayed.

router-id *A.B.C.D*

Displays neighbor information for the specified router ID.

Modes

User EXEC mode

Command Output

The **show ip ospf neighbor** command displays the following information:

Output field	Description
Port	The port through which the device is connected to the neighbor.
Address	The IP address of the port on which this device is connected to the neighbor.
Pri	The OSPF priority of the neighbor. • For multi-access networks, the priority is used during election of the Designated Router (DR) and Backup designated Router (BDR). • For point-to-point links, this field shows one of the following values: • 1 = point-to-point link • 3 = point-to-point link with assigned subnet
State	The state of the conversation between the device and the neighbor. This field can have one of the following values: • Down - The initial state of a neighbor conversation. This value indicates that there has been no recent information received from the neighbor. • Attempt - This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor. • Init - A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not

Output field	Description
	yet been established with the neighbor. (The router itself did not appear in the neighbor's Hello packet.) All neighbors in this state (or higher) are listed in the Hello packets sent from the associated interface. • 2-Way - Communication between the two routers is bidirectional. This is the most advanced state before beginning adjacency establishment. The Designated Router and Backup Designated Router are selected from the set of neighbors in the 2-Way state or greater. • ExStart - The first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. Neighbor conversations in this state or greater are called adjacencies. • Exchange - The router is describing its entire link state database by sending Database Description packets to the neighbor. Each Database Description packet has a DD sequence number, and is explicitly acknowledged. Only one Database Description packet can be outstanding at any time. In this state, Link State Request packets can also be sent asking for the neighbor's more recent advertisements. All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets. • Loading - Link State Request packets are sent to the neighbor asking for the more recent advertisements that have been discovered (but not yet received) in the Exchange state. • Full - The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network link advertisements.
Neigh Address	The IP address of the neighbor. For point-to-point links, the value is as follows: • If the **Pri** field is "1", this value is the IP address of the neighbor router's interface. • If the **Pri** field is "3", this is the subnet IP address of the neighbor router's interface.
Neigh ID	The neighbor router's ID.
Ev	The number of times the neighbor's state changed.
Opt	The sum of the option bits in the Options field of the Hello packet. This information is used by Brocade technical support. Refer to Section A.2 in RFC 2178 for information about the Options field in Hello packets.
Cnt	The number of LSAs that were retransmitted.

Examples

The following example displays information about OSPF neighbors.

```
device> show ip ospf neighbor

Port  Address       Pri  State     Neigh Address  Neigh ID    Ev Op Cnt
v10   10.1.10.1     1    FULL/DR   10.1.10.2      10.65.12.1   5  2  0
v11   10.1.11.1     1    FULL/DR   10.1.11.2      10.65.12.1   5  2  0
v12   10.1.12.1     1    FULL/DR   10.1.12.2      10.65.12.1   5  2  0
v13   10.1.13.1     1    FULL/DR   10.1.13.2      10.65.12.1   5  2  0
v14   10.1.14.1     1    FULL/DR   10.1.14.2      10.65.12.1   5  2  0
```

show ip ospf redistribute route

Displays routes that have been redistributed into OSPF.

Syntax

show ip ospf redistribute route [*A.B.C.D:M*]

Parameters

A.B.C.D:M

Specifies an IP address and mask for the output.

Modes

User EXEC mode

Examples

The following example shows sample output for the **show ip ospf redistribute route** command when no IP address and network mask are specified.

```
device> show ip ospf redistribute route

  4.3.0.0 255.255.0.0 static
  3.1.0.0 255.255.0.0 static
  10.11.61.0 255.255.255.0 connected
  4.1.0.0 255.255.0.0 static
```

The following example shows sample output for the **show ip ospf redistribute route** command when an IP address and network mask is specified.

```
device> show ip ospf redistribute route 192.213.1.0 255.255.255.254

  192.213.1.0 255.255.255.254 fwd 0.0.0.0 (0) metric 10 connected
```

show ip ospf routes

Displays OSPF calculated routes.

Syntax

show ip ospf routes [*A.B.C.D*]

Parameters

A.B.C.D

Specifies a destination IP address in dotted decimal format.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display routes that OSPF calculated. You can display all routes or you can display information about a specific route.

Command Output

The **show ip ospf routes** command displays the following information:

Output field	Description
Destination	The IP address of the route's destination.
Mask	The network mask for the route.
Path_Cost	The cost of this route path. (A route can have multiple paths. Each path represents a different exit port for the device.)
Type2_Cost	The type 2 cost of this path.
Path_Type	The type of path, which can be one of the following: • – Inter - The path to the destination passes into another area. – Intra - The path to the destination is entirely within the local area. – External1 - The path to the destination is a type 1 external route. – External2 - The path to the destination is a type 2 external route.
Adv_Router	The OSPF router that advertised the route to this device.
Link-State	The link state from which the route was calculated.
Dest_Type	The destination type, which can be one of the following: • – ABR - Area Border Router – ASBR - Autonomous System Boundary Router – Network - the network

Output field	Description
State	The route state, which can be one of the following: • – Changed – Invalid – Valid This information is used by Brocade technical support.
Tag	The external route tag.
Flags	State information for the route entry. This information is used by Brocade technical support.
Paths	The number of paths to the destination.
Out_Port	The router port through which the device reaches the next hop for this route path.
Next_Hop	The IP address of the next-hop router for this path.
Type	The route type, which can be one of the following: • – OSPF – Static Replaced by OSPF
State	State information for the path. This information is used by Brocade technical support.

Examples

The following example displays all OSPF-calculated routes.

```
device> show ip ospf route

OSPF Area 0x00000000 ASBR Routes 1:
      Destination     Mask            Path_Cost Type2_Cost Path_Type
      10.65.12.1      255.255.255.255 1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      10.65.12.1      10.65.12.1      Asbr      Valid      0          6000
      Paths Out_Port  Next_Hop        Type      State
      1     v49       10.1.49.2       OSPF      21 01
      2     v12       10.1.12.2       OSPF      21 01
      3     v11       10.1.11.2       OSPF      21 01
      4     v10       10.1.10.2       OSPF      00 00
OSPF Area 0x00000041 ASBR Routes 1:
      Destination     Mask            Path_Cost Type2_Cost Path_Type
      10.65.12.1      255.255.255.255 1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      10.65.12.1      10.65.12.1      Asbr      Valid      0          6000
      Paths Out_Port  Next_Hop        Type      State
      1     v204      10.65.5.251     OSPF      21 01
      2     v201      10.65.2.251     OSPF      20 d1
      3     v202      10.65.3.251     OSPF      20 cd
      4     v205      10.65.6.251     OSPF      00 00
OSPF Area Summary Routes 1:
      Destination     Mask            Path_Cost Type2_Cost Path_    Type
      10.65.0.0       255.255.0.0     0         0          Inter
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      10.1.10.1       0.0.0.0         Network   Valid      0          0000
      Paths Out_Port  Next_Hop        Type      State
      1     1/1       0.0.0.0         DIRECT    00 00
OSPF Regular Routes 208:
      Destination     Mask            Path_Cost Type2_Cost Path_Type
      10.1.10.0       255.255.255.252 1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      10.1.10.1       10.1.10.2       Network   Valid      0          0000
      Paths Out_Port  Next_Hop        Type      State
      1     v10       0.0.0.0         OSPF      00 00
      Destination     Mask            Path_Cost Type2_Cost Path_Type
      10.1.11.0       255.255.255.252 1         0          Intra
      Adv_Router      Link_State      Dest_Type State      Tag       Flags
      10.1.10.1       10.1.11.2       Network   Valid      0          0000
      Paths Out_Port  Next_Hop        Type      State
      1     v11       0.0.0.0         OSPF      00 00
```

show ip ospf summary

Displays summary information for all OSPF instances.

Syntax

show ip ospf summary

Modes

User EXEC mode

Examples

```
device> show ip ospf summary

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     5       2       1         12      2
```

show ip ospf traffic

Displays OSPF traffic details.

Syntax

show ip ospf traffic

Modes

User EXEC mode

Examples

The following example shows all OSPF traffic.

```
device> show ip ospf traffic

                 Packets Received         Packets Sent
Hello                          10                   10
Database                       90                   89
LSA Req                        12                   11
LSA Upd                        12                   12
LSA Ack                        12                   12
Packet Errors: None
```

show ip ospf trap

Displays OSPF trap status.

Syntax

show ip ospf trap

Modes

User EXEC mode

Examples

The following example shows all OSPF traffic.

```
device> show ip ospf trap

Interface State Change Trap:                      Enabled
Virtual Interface State Change Trap:              Enabled
Neighbor State Change Trap:                       Enabled
Virtual Neighbor State Change Trap:               Enabled
Interface Configuration Error Trap:               Enabled
Virtual Interface Configuration Error Trap:       Enabled
Interface Authentication Failure Trap:            Enabled
Virtual Interface Authentication Failure Trap:    Enabled
Interface Receive Bad Packet Trap:                Enabled
Virtual Interface Receive Bad Packet Trap:        Enabled
Interface Retransmit Packet Trap:                 Disabled
Virtual Interface Retransmit Packet Trap:         Disabled
Originate LSA Trap:                               Disabled
Originate MaxAge LSA Trap:                        Disabled
Link State Database Overflow Trap:                Disabled
Link State Database Approaching Overflow Trap:    Disabled
```

show ip ospf virtual link

Displays information about virtual links.

Syntax

show ip ospf virtual link [*index*]

Parameters

index

Shows information about all virtual links or one virtual link that you specify.

Modes

User EXEC mode

Examples

The following example shows information about all virtual links.

```
device> show ip ospf virtual link

Indx Transit Area     Router ID        Transit(sec) Retrans(sec) Hello(sec)
1    1                131.1.1.10       1            5            10
     Dead(sec)        events           state        Authentication-Key
     40               1                ptr2ptr      None
     MD5 Authentication-Key:       None
     MD5 Authentication-Key-Id:    None
     MD5 Authentication-Key-Activation-Wait-Time:      300
```

show ip ospf virtual neighbor

Displays information about virtual neighbors.

Syntax

show ip ospf virtual neighbor [*index*]

Parameters

index

Shows information about all virtual neighbors or one virtual neighbor that you specify.

Modes

User EXEC mode

Examples

The following example shows information about all virtual neighbors.

```
device> show ip ospf virtual neighbor

Indx Transit Area    Router ID      Neighbor address options
1    1               131.1.1.10     135.14.1.10       2
     Port    Address         state   events          count
     6/2     27.11.1.27      FULL    5               0
```

show ip route

Displays information about the routes through LSP tunnels.

Syntax

show ip route [*ip_addr* | *num* | **bgp** | **connected** | **import** | **isis** | **local** | **mpls-shortcut** | **nexthop** | **ospf** | **rip** | **static** | **summary** | **tags** | **vrf**]

Parameters

ip_addr

Displays the IP address.

num

Displays the route table entry whose route number corresponds to the number you specify. For example, if you want to display thr tenth row in the table, enter "10".

bgp

Displays BGP routes.

connected

Displays directly connected routes.

import

Displays imported IPv4 routes.

isis

Displays IS-IS routes.

local

Displays local IPv4 routes.

mpls-shortcut

Displays a list of installed shortcut routes (both LDP and RSVP shortcut routes).

next-hop

Displays the route next-hop table.

ospf

Displays OSPF routes.

rip

Displays RIP routes.

static

Displays static IP routes.

summary

Displays a route summary.

tags

Displays labels associated with routes.

vrf

Displays VRF routes.

Modes

User EXEC mode

Usage Guidelines

Command Output

The **show ip route** command displays the following information:

Output field	Description
Destination	The destination network of the route.
Gateway	The next-hop router.
Port	The port through which the device sends packets to reach the route's destination.
Cost	The route cost.
Type	The route type, which can be one of the following: • **B** - The route was ascertained from BGP. • **D** - The destination is directly connected to this device. • **R** - The route was ascertained from RIP. • **S** - The route is a static route. • * - The route is a candidate default route. • **O** - The route is an OSPF route. Unless you use the **ospf** option to display the route table, **O** is used for all OSPF routes. If you do not use the **ospf** option, the following type codes are used: – **O** - OSPF intra-area route (within the same area). – **IA** - The route is an OSPF inter-area route (a route that passes from one area to another area). – **E1** - The route is an OSPF external type 1 route. – **E2** - The route is an OSPF external type 2 route.

Examples

The following example displays a sample output of the **show ip route** command.

```
device# show ip route
Total number of IP routes: 1027
 Type codes - B:BGP  D:Disconnected  S:Static  R:RIP  O:OSPF; Cost-Dist/Metric
   Destination    Gateway     Port          Cost      Type
1  10.1.1.1/32    DIRECT      loopback 1    0/0       D
2  10.1.2.1/32    DIRECT      loopback 2    0/0       D
3  10.1.3.1/32    DIRECT      loopback 3    0/0       D
4  10.2.2.2/32    10.0.0.2    eth 1/1       110/10    O
5  10.3.3.3/32    10.0.0.2    eth 1/1       110/12    O
   10.3.3.3/32    10.8.0.2    eth 1/4       110/12    O
6  10.4.4.4/32    10.8.0.2    eth 1/4       110/10    O
7  10.5.1.5/32    10.5.5.5    lsp(LDP)      200/0     B
8  10.5.3.5/32    10.5.5.5    lsp(LDP)      200/0     B
9  10.5.5.5/32    10.0.0.2    eth 1/1       110/13    O
   10.5.5.5/32    10.8.0.2    eth 1/4       110/13    O
10 10.6.1.6/32    10.6.6.6    lsp(LDP)      200/0     B
11 10.6.1.6/32    10.6.6.6    lsp(LDP)      200/0     B
12 10.6.3.6/32    10.6.6.6    lsp(LDP)      200/0     B
13 10.6.4.6/32    10.6.6.6    lsp(LDP)      200/0     B
14 10.6.5.6/32    10.6.6.6    lsp(LDP)      200/0     B
15 10.6.6.6/32    10.0.0.2    eth 1/1       110/14    O
   10.6.6.6/32    10.8.0.2    eth 1/4       110/14    O
```

The following example displays a sample output of the **show ip route** command using the **mpls-shortcut** option.

```
device# show ip route mpls-shortcut
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area  1:External Type 1  2:External Type 2  s:sham link
STATIC Codes - d:DHCPv6
     Destination    Gateway       Port      Cost   Type  Uptime scr-vrf
```

History

Release version	Command history
6.0.0	This command was modified to include the keyword **mpls-shortcut**.

show ip static-arp

Displays port, VPLS-ID, VLAN, and VPLS peer information.

Syntax

show ip static-arp [*ip_addr ip_mask*] | *num* | [**ethernet** *slot* **/** *port*] | [**mac-address** *mac_addr*] | [**vlan** *vlan_id*] | [**vrf** *vrf_name*]

Parameters

ip_addr
Specifies the selected IP address.

ip_mask
Specifies the selected IP network mask.

num
Specifies the number of entries to skip.

ethernet *slot/port*
Displays the specified ethernet port.

mac-address *mac_addr*
Displays the specified mac address in hexadecimal (xxxx.xxxx.xxxx).

vlan *vlan_id*
Displays the specified VLAN. A choice of zero (0) signifies

vrf *vrf_name*
Displays static ARP entries belonging to a given VRF instance.

Modes

EXEC mode

Usage Guidelines

Command Output

The **show ip static-arp** command displays the following information:

Output field	Description
Index	The number of this entry in the table. You specify the entry number when you create the entry.
IP Address	The IP address of the device.
MAC Address	The MAC address of the device.
Port/VLAN	Port and VLAN ID.
ESI	*Ethernet Service Instance (ESI)* associated with this entry, if any.

Output field	Description
Vpls-Vlan: Port/Vpls-Peer	Shows the VPLS ID under the 'Port' field when applicable. The 'Port' field for the VPLS VE ARP displays in the format '*:vpls-vlan: port' or '*: vpls-peer_ip_address'

Examples

The following example shows the **show ip static-arp** command output.

```
device(config)# show ip static-arp
Total no. of entries: 2
Index  IP Address    MAC Address     Port/VLAN  ESI  Vpls-Vlan:Port/Vpls-Peer
1      10.10.10.10   0000.0033.4444  100
2      10.11.11.11   0000.0066.7777  4/1
3      10.12.12.12   0000.0023.4343                  *:21:3/2
4      10.26.5.12    0000.00F3.4343                  *:1.2.3.105
```

show ip vrrp

Displays information about IPv4 Virtual Router Redundancy Protocol (VRRP) sessions.

Syntax

show ip vrrp [**brief**]

show ip vrrp [**ethernet** *slot*/*port* | **ve** *num*]

show ip vrrp [**statistics** [**ethernet** *slot*/*port* | **ve** *num*]]

show ip vrrp [**ve** *num* [**vrid** *VRID*]]

show ip vrrp [**vrid** *VRID* [**ethernet** *slot*/*port* | **ve** *num*]]

Parameters

brief
Displays summary information about the VRRP session.

ethernet *slot port*
Displays IPv4 VRRP information only for the specified port. A forward slash "/" must be entered between the *slot* and *port* variables.

statistics
Displays statistical information about the VRRP session.

ve *num*
Displays IPv4 VRRP information only for the specified virtual Ethernet port.

vrid *VRID*
Displays IPv4 VRRP information only for the specified virtual-group ID.

Modes

User EXEC mode

Usage Guidelines

Use this command to display information about IPv4 VRRP sessions, either in summary or full-detail format. You can also specify a virtual group or interface for which to display output.

This command supports IPv4 VRRP. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Command Output

The **show ip vrrp** command displays the following information.

Output field	Description
Total number of VRRP routers defined	The total number of virtual routers configured and currently running on this Brocade device. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers.
Interface	The interface on which VRRP or VRRP-E is configured. If VRRP or VRRP-E is configured on multiple interfaces, information for each interface is listed separately.
VRID	The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row.
Current Priority	The current VRRP or VRRP-E priority of this Brocade device for the virtual router.
Flags Codes	Whether the backup preempt mode is enabled and which version of VRRP is enabled. If the backup preempt mode is enabled, this field contains a "P". If the mode is disabled, this field is blank. • P:Preempt • 2:V2—VRRP Version 2 • 3:V3—VRRP Version 3 • S:Short-Path-Fwd—Short-path forwarding is enabled
State	This Brocade device's VRRP state for the virtual router. The state can be one of the following: • Init—The virtual router is not enabled (activated). If the state remains Init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other. If the state is Init and the mode is incomplete, make sure that you have specified the IP address for the virtual router. • Backup—This Brocade device is a backup for the virtual router. • Master—This Brocade device is the master for the virtual router.
Master IP Address	The IP address of the router interface that is currently the Master for the virtual router. If the IP address is assigned on this device, "Local" is displayed here.
Backup IP Address	The IP addresses of the router interfaces that are currently backups for the virtual router. If the IP address is not known in th routing table, "Unknown" is displayed here.
Virtual IP Address	The virtual IP address that is being backed up by the virtual router.

Examples

The following example displays VRRP session information in summary format.

```
device(config)# show ip vrrp brief

Total number of VRRP routers defined: 2
Flags Codes - P:Preempt 2:V2 3:V3 S:Short-Path-Fwd
Inte- VRID  Current  Flags    State   Master IP Backup IP  Virtual IP
rface       Priority                 Address   Address    Address
-------------------------------------------------------------------------
1/1   10    255      P2-      Master  Local     Unknown    10.30.30.2
1/3   13    100      P2-      Master  Local     Unknown    10.13.13.3
```

The following example displays IPv4 VRRP configuration information about VRID 1.

```
device# show ip vrrp vrid 1

Interface 1/6
----------------
auth-type no authentication
VRID 1 (index 1)
interface 1/6
state master
administrative-status enabled
version v2
mode owner
virtual mac aaaa.bbbb.cccc (configured)
priority 255
current priority 255
track-priority 40
hello-interval 1 sec
backup hello-interval 6
track-port tunnel 1 (UP)
```

show ip vrrp-extended

Displays information about IPv4 Virtual Router Redundancy Protocol Extended (VRRP-E) sessions.

Syntax

show ip vrrp-extended [**brief**]

show ip vrrp-extended [**ethernet** *slot*/*port* | **ve** *num*]

show ip vrrp-extended [**statistics** [**ethernet** *slot*/*port* | **ve** *num*]]

show ip vrrp-extended [**ve** *num* [**vrid** *VRID*]]

show ip vrrp-extended [**vrid** *VRID* [**ethernet** *slot*/*port* | **ve** *num*]]

Parameters

brief

Displays summary information about the VRRP-E session.

ethernet *slot port*

Displays IPv4 VRRP-E information only for the specified port. A forward slash "/" must be entered between the *slot* and *port* variables.

ve *num*

Displays IPv4 VRRP-E information only for the specified virtual Ethernet port.

statistics

Displays statistical information about the VRRP-E session.

vrid *VRID*

Displays IPv4 VRRP-E information only for the specified virtual-group ID.

Modes

User EXEC mode

Usage Guidelines

Use this command to display information about IPv4 VRRP-E sessions, either in summary or full-detail format. You can also specify a virtual group or interface for which to display output.

This command supports IPv4 VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

This command can be entered in any mode on the device.

Command Output

The **show ip vrrp-extended** command displays the following information.

Output field	Description
Total number of VRRP-E routers defined	The total number of virtual routers configured and currently running on this Brocade device. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers.
Interface	The interface on which VRRP or VRRP-E is configured. If VRRP or VRRP-E is configured on multiple interfaces, information for each interface is listed separately.
VRID	The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row.
Current Priority	The current VRRP or VRRP-E priority of this Brocade device for the virtual router.
Flags	Whether the backup preempt mode is enabled. If the backup preempt mode is enabled, this field contains a "P". If the mode is disabled, this field is blank. • P:Preempt 2:V2 3:V3 • 2: implies VRRP Version2 • 3: implies VRRP Version3
State	This Brocade device's VRRP state for the virtual router. The state can be one of the following: • Init—The virtual router is not enabled (activated). If the state remains Init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other. If the state is Init and the mode is incomplete, make sure that you have specified the IP address for the virtual router. • Backup—This Brocade device is a backup for the virtual router. • Master—This Brocade device is the master for the virtual router.
Master IP Address	The IP address of the router interface that is currently the Master for the virtual router. If the IP address is assigned on this device, "Local" is displayed here.
Backup IP Address	The IP addresses of the router interfaces that are currently backups for the virtual router. If the IP address is not known in th routing table, "Unknown" is displayed here.
Virtual IP Address	The virtual IP address that is being backed up by the virtual router.

Examples

The following example displays summary information for a VRRP-E session.

```
device# show ip vrrp-extended brief

Total number of VRRP-E routers defined: 2
Flags Codes - P:Preempt 2:V2 3:V3 S:Short-Path-Fwd
Inte- VRID  Current  Flags    State   Master IP Backup IP  Virtual IP
rface       Priority                 Address   Address    Address
-------------------------------------------------------------------
Ve 1  2     255      P2-      Master  Local     10.30.20.2 10.30.30.2
Ve 3  4     100      P2-      Backup  Local     10.30.20.2 10.30.30.2
```

The following example displays the number of configured virtual IPv4 addresses for each VRRP-E router instance and the virtual IPv4 addresses when the VRRP-E multiple virtual IP addresses feature is configured.

```
device# show ip vrrp-extended brief

Total number of VRRP-Extended routers defined: 3
Flags Codes - P:Preempt 2:V2 3:V3
Short-Path-Fwd Codes - ER: Enabled with revertible option, RT: reverted,
                       NR: not reverted

Intf VRID Curr Flags State  MasterIP BackupIP (No) VirtualIP  Short-   Track MCT
          Prio              Address  Address       Address    Path-Fwd VPLS-State
-------------------------------------------------------------------------------
1/1  1    100  P2    Master Local    Unknown   (7) 10.10.10.10 Enabled Disable
                                                   10.20.20.20
                                                   10.30.30.30
                                                   10.40.40.40
                                                   10.50.50.50
                                                   10.60.60.60
                                                   10.70.70.70
```

The following example displays detailed information for a VRRP-E backup device.

```
device(config)# show ip vrrp-extended

Total number of vrrp-extended routers defined: 1
Interface v10
---------------
auth-type no authentication
VRID 10 (index 1)
interface v10
state backup
administrative-status enabled
mode non-owner(backup)
virtual mac 02e0.52a0.c00a
priority 50
current priority 50
track-priority 5
hello-interval 1 sec
backup hello-interval 60 sec
slow-start timer (configured) 30 sec
advertise backup disabled
dead-interval 3600 ms
preempt-mode true
virtual ip address 10.10.10.254
next hello sent in 1000ms
track-port 1/1 (up)
master router 10.10.10.4 expires in 3.1 sec
short-path-forwarding enabled
```

The following example displays IPv4 VRRP-E statistics. The “received vrrp-extended packets with unknown or inactive vrid” shows the number of packets that contain virtual router IDs that are not configured on the device or its interface.

```
device> show ip vrrp-extended statistics

Global VRRP-Extended statistics
-------------------------------
- received vrrp-extended packets with checksum errors = 0
- received vrrp-extended packets with invalid version number = 0
- received vrrp-extended packets with unknown or inactive vrid = 1480
Interface v10
-----------------
VRID 1
- number of transitions to backup state = 1
- number of transitions to master state = 1
- total number of vrrp-extended packets received = 0
. received backup advertisements = 0
. received packets with zero priority = 0
. received packets with invalid type = 0
. received packets with invalid authentication type = 0
. received packets with authentication type mismatch = 0
. received packets with authentication failures = 0
. received packets dropped by owner = 0
. received packets with ip ttl errors = 0
. received packets with ip address mismatch = 0
. received packets with advertisement interval mismatch = 0
. received packets with invalid length = 0
- total number of vrrp-extended packets sent = 2004
. sent backup advertisements = 0
. sent packets with zero priority = 0
- received arp packets dropped = 0
- received proxy arp packets dropped = 0
- received ip packets dropped = 0
```

The following example displays IPv4 VRRP-E configuration information about VRID 1.

```
device# show ip vrrp-extended vrid 1

Interface 1/1
----------------
auth-type md5-authentication
VRID 1 (index 1)
interface 1/1
state master
administrative-status disabled
mode non-owner(backup)
virtual mac aaaa.bbbb.cccc (configured)
priority 100
current priority 100
track-priority 5
hello-interval 1 sec
backup hello-interval 60 sec
slow-start timer (configured) 30 sec
advertise backup disabled
dead-interval 0 ms
preempt-mode true
virtual ip address 10.20.1.100
short-path-forwarding disabled
```

The following example displays group member information for the VRRP-E scaling feature for VRID 1. Only partial output is displayed.

```
device(config)# show ip vrrp-extended vrid 1

VRID 1 (index 1)
 interface 1/1
 state master
. administrative-status enabled
.
.
 group-member count 3
 group-members
   ethernet 1/2 vrid 2
   ethernet 1/2 vrid 3
   ethernet 1/2 vrid 4
```

The following example displays group master information for the VRRP-E scaling feature for interface Ethernet 1/1 and VRID 2. Only partial output is displayed.

```
device(config)# show ip vrrp-extended ethernet 1/1 vrid 2

VRID 2 (index 2)
 interface 1/2
 state master
 administrative-status enabled
.
.
.
 short-path-forwarding disabled
 group-master ethernet 1/1 vrid 1
```

History

Release version	Command history
05.8.00	This command was modified to add new output for the VRRP-E scaling using logical groups and VRRP-E multiple virtual IP addresses features.

show ipsec egress-config

Displays egress configuration register contents for IPsec.

Syntax

show ipsec egress-config

Modes

Privileged EXEC mode

Examples

The following example displays **show ipsec egress-config** command output.

```
device# show ipsec egress-config

 IPSec Egress Configuration
   Packet with Seq no maxout error:         Packet Drop
   Packet with NHT entry error:             Packet Drop
   Packet with unsupported IP header error: Packet Drop
   Packet with invalid SPI error:           Packet Drop
   Non-IP packet for Encapsulation:         Packet Drop
   Packet encryption:                       Enabled
   IP header check:                         Enabled
```

History

Release version	Command history
05.8.00	This command was introduced.

show ipsec egress-spi-table

Displays the software copy and the details of the IPsec egress SPI lookup table entry. This command supports IPsec IPv4 and IPv6.

Syntax

show ipsec egress-spi-table

Modes

Privileged EXEC mode

Examples

The following example shows the output for an IPsec egress SPI lookup table.

This example is for IPsec IPv4.

```
device#show ipsec egress-spi-table
 Egress SPI Lookup Table (total entries: 5)
idx  spi        spa             dpa             tnnl
   1 0x7883db6f 52.54.112.52    52.54.112.54    112
   2 0xefeaffe5 52.54.111.52    52.54.111.54    111

device#show ipsec egress-spi-table 2
 egress-spi-id: 2
  SPA: 0x00000000 00000000 00000000 34366f34
  DPA: 0x00000000 00000000 00000000 34366f36
  Mode: IPv4(Tunnel)  ReplayCheck: Enabled  ESN_Support: Disabled
  TC/TOS: 0(ValidBit: UnSet)  HopLimit/TTL: 255
  SPI: 0xefeaffe5  Salt: 0x88876d98  SequenceNumber: 0x0000000000000002
  ReplayVector: 0x0000000000000001
  AES-256-GCM-KEY: 0x8478313e48f17e2ae1554db2f46762d7865a7ab2a51b4760a6e0c6e522e87988
```

History

Release version	Command history
05.8.00	This command was introduced.
05.9.00	This command was modified to add support for IPsec IPv6.

show ipsec error-count

Displays the number of packets encountered with errors, while processing IPsec packets.

Syntax

show ipsec error-count

Modes

Privileged EXEC mode

Examples

The following example displays **show ipsec error-count** command output.

```
device#show ipsec error-count
  Ingress Replay Error Count                                  : 0
  Ingress Authentication Error Count                          : 0
  Ingress Pkt Length not in 4byte boundry Error Count         : 0
  Ingress Pkt ESP header not in 16byte boundry Error Count    : 0
  Ingress Pkt Drop due to Tunnel Mis-match Error Count        : 0
  Ingress Pkt EOF before indicated by IP pkt length Error Count: 0
  Ingress Pkt De-encapsulation Error Count                    : 0
  Ingress Pkt ESP header in fragmented IP pkt Error Count     : 0
  Egress Invalid SPI table entry Error Count                  : 0
  Egress non-IP Pkt Encapsulation Error Count                 : 0
  Egress Nexthop Table Error Count                            : 0
  Egress Unsupported Pkt Encapsulation Error Count            : 0
  Egress Sequence Number Max-out Error Count                  : 0
```

History

Release version	Command history
05.8.00	This command was introduced.

show ipsec ingress-config

Displays ingress configuration register contents for IPsec.

Syntax

show ipsec ingress-config

Modes

Privileged EXEC mode

Examples

The following example displays **show ipsec ingress-config** command output.

```
device#show ipsec ingress-config

 IPSec Ingress Configuration
   Packet with encapsulation error:         Send to CPU
   Packet with tunnel check error:          Send to CPU
   Packet with replay check error:          Send to CPU
   Packet with authentication error:        Send to CPU
   Packet with fragmentation error:         Send to CPU
   Packet with IP length error:             Send to CPU
   Hash based on SPI used as Ingress SPI table index
   Decapsulation:                           Enabled
   Decryption:                              Enabled
   Next header check:                       Enabled
   IPDA check:                              Enabled
   IPSA check:                              Enabled
   Early EoF check:                         Enabled
   IP length not in 4B boundary check:      Disabled
   ESP length not in 16B boundary check:    Enabled
   IP fragmentation check:                  Enabled
   Authentication check:                    Enabled
```

History

Release version	Command history
05.8.00	This command was introduced.

show ipsec ingress-spi-table

Displays the software copy and the details of the IPsec ingress SPI lookup table entry. This command supports IPsec IPv4 and IPv6.

Syntax

show ipsec ingress-spi-table

Modes

Privileged EXEC mode

Examples

The following example shows the output for an IPsec ingress SPI lookup table.

This example is for IPsec IPv4.

```
device#show ipsec ingress-spi-table
 Ingress SPI Lookup Table (total entries: 5)
idx  spi        spa             dpa             tnnl
   1 0x6e2d9ba8 52.54.112.54    52.54.112.52    112
   2 0x3b191431 52.54.111.54    52.54.111.52    111
device#show ipsec ingress-spi-table 2
 ingress-spi-id: 2
  SPA: 0x00000000 00000000 00000000 34366f36
  DPA: 0x00000000 00000000 00000000 34366f34
  Mode: IPv4(Tunnel)  ReplayCheck: Enabled  ESN_Support: Disabled
  SPI: 0x3b191431  Salt: 0xf1db462b  SequenceNumber: 0x0000000000dc042a
  ReplayVector: 0xffffffffffffffff
  AES-256-GCM-KEY: 0xe5649a5cf623dcd134cbf280bfd95eb390719557bd1663d748aece2c6b8eacb0
```

History

Release version	Command history
05.8.00	This command was introduced.
05.9.00	This command was modified to add support for IPsec IPv6.

show ipsec policy

Displays information about the IP security (IPsec) policy database.

Syntax

show ipsec policy

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

Examples

The following example shows how to display the IPsec policy database.

```
device# show ipsec policy

             IPSEC Security Policy Database(Entries:2)
PType  Dir Proto Source(Prefix:TCP/UDP Port)
                 Destination(Prefix:TCP/UDPPort)
  SA: SPDID(vrf:if) Dir Encap SPI        Destination
use    in  OSPF  FE80::/10:any
                 ::/0:any
  SA: 0:v2          in  ESP   400        FE80::

use    out OSPF  FE80::/10:any
                 ::/0:any
  SA: 0:v2          out ESP   400        ::
use    in  all    0.0.0.0/0:any
                  0.0.0.0/0:any
  SA: 1:Tun1         in   ESP  0xBD481319 10.2.10.2
use    out  all    0.0.0.0/0:any
                   0.0.0.0/0:any
  SA: 1:Tun1         out  ESP  0x9EAB77D6 10.2.10.2
```

History

Release version	Command history
5.8.00	This command was introduced.

show ipsec profile

Displays configuration information about IP security (IPsec) profiles.

Syntax

show ipsec profile [*profile-name*]

Parameters

profile-name

Specifies the name of an IPsec profile.

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

When an IPsec profile is not specified, this command displays configuration information for all IPsec profiles.

Command Output

The **show ipsec profile** command displays the following information:

Output field	Description
Name	The name of an IPsec profile.
Description	A description of the IPsec profile.
Ike Profile	The name of the IKEv2 profile that is attached to this IPsec profile.
Lifetime	The lifetime period (in minutes) for an IPsec SA. The range is from 10 through 1440. The default value is 480 minutes (8 hours). A value of 0 indicates that the IPsec SA remains up indefinitely.
Anti-replay service	
Replay window size	
DH group	The Diffie-Hellman group that is used for IKEv2 negotiations.
Proposal	The name of any IPsec proposals that are attached to this IPsec profile.

Examples

The following example shows how to display IPsec profile configuration information.

```
device# show ipsec profile

Name                : red
Ike Profile         : red
Lifetime            : 28800
Anti-replay service : Enabled
 Replay window size : 64
DH group            : None
Proposal            : red
```

History

Release version	Command history
05.8.00	This command was introduced.

show ipsec proposal

Displays configuration information about IP security (IPsec) proposals.

Syntax

show ipsec proposal [*proposal-name*]

Parameters

proposal-name

Specifies the name of an IPsec proposal.

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

When an IPsec proposal is not specified, this command displays configuration information for all IPsec proposals.

Command Output

The **show ipsec proposal** command displays the following information:

Output field	Description
Name	The name of the IPsec proposal.
Protocol	The transform type.
Encryption	A list of encryption algorithms that are supported.
Authentication	The authentication method for data traffic.
ESN	The Extended Sequence Number (ESN) status.
Mode	The packet encapsulation mode that is supported.

Examples

The following example shows how to display configuration information for an IPsec proposal named prop_red.

```
device# show ipsec proposal prop-red

   Name          : prop_red
   Protocol      : ESP
   Encryption    : aes-gcm-256
   Authentication: NULL
   ESN           : Enable
   Mode          : Tunnel
```

History

Release version	Command history
05.8.00	This command was introduced.

show ipsec sa

Displays information about the current IPsec Security Associations (SA) that exist on the device or on the IPsec interface. This command supports IPsec IPv4 and IPv6.

Syntax

show ipsec sa [**address** [*address* | *ipv6-address*] | **identity** *id* | **interface** *name* | **peer** *ip-address*] [**detail**]

Parameters

address *address*
(Optional) Specifies the IPv4 address of the IPsec interface.

address *ipv6-address*
(Optional) Specifies the IPv6 address of the IPsec interface.

identity *id*
(Optional) Specifies the IPsec identity ID value.

interface *name*
(Optional) Specifies the IPsec interface name.

peer *ip-address*
(Optional) Specifies the IP address of the IPsec interface.

detail
(Optional) Specifies to include details of the IPsec SA in the output.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not include the optional **detail** parameter, only the basic information about the IPsec SA is included in the output.

Examples

These examples are for IPsec IPv4.

The following example shows output for command **show ipsec sa** for the an IPsec SAs on the device.

```
device# show ipsec sa
            IPSEC Security Association Database(Entries:2)
SPDID(vrf:if) Dir Encap SPI        Destination
  AuthAlg  EncryptAlg Status Mode
0:v2          out ESP   400        ::
  sha1     Null       ACT    TRAN
0:v2          in  ESP   400        FE80::
  sha1     Null       ACT    TRAN
1:Tun1         in   ESP   0xBD481319   1.2.10.2
  Null      AES-GCM-256 ACT     TNL
1:Tun1         out  ESP   0x9EAB77D6   1.2.10.2
  Null      AES-GCM-256 ACT     TNL
```

The following example shows output for command **show ipsec sa <ipaddress> detail** for the IPsec SAs set up on interface 1.2.10.2.

```
device# show ipsec sa address 1.2.10.2 detail
Total ipsec SAs: 2

0:
    interface           : tnl 1
     Local address: 1.2.45.1/500, Remote address: 1.2.45.2/500
     Inside vrf: default-vrf
     Local identity (addr/mask/prot/port): address(0.0.0.0/0/0/0)
     Remote identity(addr/mask/prot/port): address(0.0.0.0/0/0/0)
     DF-bit: clear
     Profile-name: red
     DH group: none
     Direction: inbound, SPI: 0x0000004b
     Mode: tunnel,
     Protocol: esp, Encryption: gcm-256, Authentication: null
     ICV size: 16 bytes
     lifetime(sec): Expiring in (4606816/3576)
     Anti-replay service: Enabled, Replay window size: 0
     Status: ACTIVE
     slot Assigned 0
     nht_index 0000ffff
     Is tunnel NHT: false
1:
    interface           : tnl 1
     Local address: 1.2.45.1/500, Remote address: 1.2.45.2/500
     Inside vrf: default-vrf
     Local identity (addr/mask/prot/port): address(0.0.0.0/0/0/0)
     Remote identity(addr/mask/prot/port): address(0.0.0.0/0/0/0)
     DF-bit: clear
     Profile-name: red
     DH group: none
     Direction: inbound, SPI: 0x0000009c
     Mode: tunnel,
     Protocol: esp, Encryption: gcm-256, Authentication: null
     ICV size: 16 bytes
     lifetime(k/sec): Expiring in (4606816/3576)
     Anti-replay service: Enabled, Replay window size: 0
     Status: ACTIVE
     slot Assigned 0
     nht_index 00000004
     Is tunnel NHT: true
```

History

Release version	Command history
05.8.00	This command was introduced.
05.9.00	This command was modified to add support for IPsec IPv6.

show ipsec statistics

Displays IPsec Security Association (SA) statistics.

Syntax

show ipsec statistics [**tunnel** *tunnel-id*]

Parameters

tunnel*tunnel-id*

Specifies the IPsec tunnel ID value.

Modes

Privileged EXEC mode

Command Output

The **show ipsec statistics** command displays the following information:

Output field	Description
IPSecurity Statistics	Displays the total current and total inbound as well as outbound security association statistics.
IPSecurity Packet Statistics	Displays the total inbound, outbound and dropped packets.
IPSecurity Error Statistics	Displays the total packet errors, such as the authentication, replay, receive, policy and send errors.

The **show ipsec statistics tunnel** command displays the following information:

Output field	Description
RxPkts	The number of packets received on the interface.
RxBytes	The volume of data (in bytes) transmitted on the interface.
TxPkts	The number of packets transmitted by the interface.
TxBytes	The volume of data (in bytes) transmitted by the interface.
RxMcPkts	The number of multicast packets received on the interface.
TxMcPkts	The number of multicast packets transmitted by the interface.

Examples

The following example displays the IPsec SA statistics.

```
device# show ipsec statistics
                      IPSecurity Statistics
ipsecEspCurrentInboundSAs 1          ipsecEspTotalInboundSAs:  1
ipsecEspCurrentOutboundSA 1          ipsecEspTotalOutboundSAs: 1
                    IPSecurity Packet Statistics
ipsecEspTotalInPkts:      0          ipsecEspTotalInPktsDrop:  0
ipsecEspTotalOutPkts:     7
                    IPSecurity Error Statistics
ipsecAuthenticationErrors 0
ipsecReplayErrors:        0          ipsecPolicyErrors:        0
ipsecOtherReceiveErrors:  0          ipsecSendErrors:          0
ipsecUnknownSpiErrors:    0
```

The following example displays the **show ipsec statistics tunnel** command output.

```
device# show ipsec statistics tunnel
#    Tnnl  RxPkts     RxBytes            TxPkts     TxBytes       RxMcPkts      TxMcPkts
1    1     1393       219574             3696386    510126444       546             321
```

The following example displays the **show ipsec statistics tunnel** command output for tunnel 1.

```
device# show ipsec statistics tunnel 1
 IPSec tunnel 1 statistics:
  RxPkts:       1399                 TxPkts:   3714027
  RxBytes:      220522               TxBytes:  512560982
  Multicast Packet Statistics:
  RxPkts:       5394                 TxPkts:   67
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00	This command was modified to include the **show ipsec statistics tunnel** command output.

show ip-tunnels

Displays information about the configured and valid IPsec tunnels (IPv4 IPsec and IPv6 IPsec) on the device. The information includes the number of the tunnels, source and destination IP addresses, whether tunnels statistics collection is enabled, the protection profile, the spi-idx and more.

Syntax

show ip-tunnels

Modes

Privileged EXEC mode

Command Output

The **show ip-tunnels** command displays the following information:

This field...	Displays...
IPv6 tnnl x *UP* | *DOWN*	The status of the interface for manual IPv6 tunnel interface x can be one of the following: • UP - The tunnel interface is functioning properly. • DOWN - The tunnel interface is not functioning and is down.
GRE tnnl x UP or DOWN	The status of the interface for GRE tunnel interface x can be one of the following: • UP - The tunnel interface is functioning properly. • DOWN - The tunnel interface is not functioning and is down.
GRE Session Enforce	Shows whether the global GRE session enforce feature is enabled. The output is one of the following: TRUE - the feature is enabled. FALSE - the feature is disabled.
IPv6 Session Enforce	Shows whether the global IPv6 session enforce feature is enabled. The output is one of the following: TRUE - the feature is enabled. FALSE - the feature is disabled.
IP Tunnel Statistics collection	Shows whether the collection of tunnel statistics is enabled. The enable or disable is a global setting that applies to both directions of GRE and manual IPv6 tunnels (unicast and multicast).
src_ip	The tunnel source can an IPv4 address.
dst_ip	The tunnel destination can an IPv4 address.
TTL	The TTL value configured for the outer IP header. The range for TTLs is 1 - 255.
TOS	The TOS value configured for the outer IP header. The range for TOS values is 1 - 255.
NHT	The nextHop Table index value.

This field...	Displays...
MTU	The setting of the IPv6 maximum transmission unit (MTU).

Examples

The following example shows the protection profile and spi-idx for the IPsec tunnels. This example is for IPsec IPv4.

```
device# show ip-tunnels
# of Configured Tunnels : 1, GRE Session Enforce: FALSE, IPv6 Session Enforce: FALSE,
   IP Tunnel Statistics collection Disabled
IPSec IPv4 tnnl 10 UP   : src_ip 1.1.1.1, dst_ip 1.1.1.2
   TTL 255, TOS 0, NHT 1, MTU 1431
  ipsec protection profile : abcd
        egress-spi-idx: 0

device# show ip-tunnels

# of Valid Tunnels : 2, GRE Session Enforce: FALSE, IPv6 Session Enforce: FALSE
   IP Tunnel Statistics collection  Disabled
IPSec IPv4 tnnl 10 UP : src_ip 1.1.1.1, dst_ip 1.1.1.2, TTL 255, TOS 0
 nht 1, mtu 1431, nht_visited 1, ingresspram_visited 0, arp_index 0x00000001
 PRAM-PPCR2:1: SrcIngressChk 0xffffffff
  ipsec protection profile : abcd
  egress-spi-idx: 1   ingress-spi-idx: 1
```

History

Release version	Command history
5.8.00	This command was introduced.
5.9.00	This command was modified to add support for IPv6.

show ipv6 access-list bindings

Displays all IPv6 access-lists bound to different interfaces. This includes both rule-based ACL and receive access-control list (rACL) information

Syntax

show ipv6 access-list bindings

Modes

User EXEC node

Usage Guidelines

Examples

The following example displays all IPv6 access-list bindings.

```
device(config)# show ipv6 access-list bindings
!
ipv6 receive access-list b1 sequence 11
ipv6 receive access-list b2 sequence 12
!
```

History

Release	Command History
5.6.00	This command was introduced.

show ipv6 access-list receive accounting

Displays accounting information for an IPv6 receive access-control list (rACL).

Syntax

show ipv6 access-list receive accounting { **brief** | **name** *acl-name* }

Parameters

brief

Displays IPv6 rACL accounting information in brief.

name *acl-name*

Specifies the name of a receive access-control list.

Modes

User EXEC mode

Examples

The following example displays rACL accounting information for the ACL "b1".

```
device(config)# show ipv6 access-list receive accounting name b1
IPv6 Receive ACL Accounting Information:
IPv6 Receive ACL b1
ACL hit count for software processing (accum)                    0
HW counters:
    0: permit tcp any host 2000::2
       Hit count: (1 sec)                   0   (1 min)                   0
                  (5 min)                   0   (accum)                   0
    1: permit udp any host 1000::1
       Hit count: (1 sec)                   0   (1 min)                   0
                  (5 min)                   0   (accum)                   0
```

History

Release	Command History
5.6.00	This command was introduced.

show ipv6 bgp

Displays entries in the BGP4+ routing table.

Syntax

show ipv6 bgp

show ipv6 bgp *ipv6-prefix /prefix-length*

show ipv6 bgp *ipv6-prefix /prefix-length* **longer-prefixes**

Parameters

ipv6-prefix

Specifies an IPv6 network number.

/prefix-length

Specifies the length of the IPv6 prefix.

longer-prefixes

Displays routes that match a specified or longer BGP prefix.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp** command displays the following information:

Output field	Description
Total number of BGP Routes (appears in display of all BGP routes only)	The number of routes known by the device.
Number of BGP Routes matching display condition (appears in display that matches specified and longer prefixes)	The number of routes that matched the display parameters you entered. This is the number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the left column of the display, to the left of each route. The status codes are described in the command's output.
Origin codes	A character the display uses to indicate the route's origin. The origin code appears to the right of the AS path (Path field). The origin codes are described in the command's output.
Network	The network prefix and prefix length.
Next Hop	The next-hop router for reaching the network from the device.
MED	The value of the route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for this route relative to other routes in the local AS. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.

Output field	Description
Path	The route's AS path.

Examples

The following example displays sample output from the **show ipv6 bgp** command.

```
device> show ipv6 bgp

Total number of BGP Routes: 2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        Metric LocPrf Weight Path
*>  2001:db8::/32      ::              1      100    32768  ?
*>  2001:db8:1234::/48 ::              1      100    32768  ?
```

This example displays sample output from the **show ipv6 bgp** command, showing information for prefix 2001:db8::/32, when the **longer-prefixes** keyword is used.

```
device> show ipv6 bgp 2001:db8::/32 longer-prefixes

Number of BGP Routes matching display condition : 3
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED LocPrf Weight Path
*>  2001:db8::/32      ::              1      100    32768  ?
*>  2001:db8:1234::/48 ::              1      100    32768  ?
*>  2001:db8:e0ff::/48 ::              1      100    32768  ?
       Route is advertised to 1 peers:
        2001:db8:4::110(65002)
```

show ipv6 bgp attribute-entries

Displays BGP4+ route-attribute entries that are stored in device memory.

Syntax

show ipv6 bgp attribute-entries

Modes

User EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4+ attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4+ route-attribute entries that are stored in device memory.

Command Output

The **show ipv6 bgp attribute-entries** command displays the following information:

Output field	Description
Total number of BGP Attribute Entries	The number of entries contained in the device's BGP4+ route-attribute entries table.
Next Hop	The IPv6 address of the next hop router for routes that have this set of attributes.
MED	The cost of the routes that have this set of attributes.
Origin	The source of the route information. The origin can be one of the following: • EGP - The routes with this set of attributes came to BGP4+ through EGP. • IGP - The routes with this set of attributes came to BGP4+ through IGP. • INCOMPLETE - The routes came from an origin other than one of the above. For example, they may have been redistributed from OSPFv3 or RIPng. When BGP4+ compares multiple routes to a destination to select the best route, IGP is preferred over EGP, and both are preferred over INCOMPLETE.
Originator	The originator of the route in a route-reflector environment.
Cluster List	The route-reflector clusters through which this set of attributes has passed.
Aggregator	Aggregator information: • AS Number shows the AS in which the network information in the attribute set was aggregated. This value applies only to aggregated routes and is otherwise 0. • Router-ID shows the router that originated this aggregator.
Atomic	Whether the network information in this set of attributes has been aggregated and this aggregation has resulted in information loss: • TRUE - Indicates information loss has occurred • FALSE - Indicates no information loss has occurred • None - Indicates this attribute is not present.

Output field	Description
	NOTE Information loss under these circumstances is a normal part of BGP4+ and does not indicate an error.
Local Pref	The degree of preference for routes that use this set of attributes relative to other routes in the local AS.
Communities	The communities that routes with this set of attributes are in.
AS Path	The ASs through which routes with this set of attributes have passed. The local AS is shown in parentheses.
Address	For debugging purposes only.
Hash	For debugging purposes only.
Reference Counts	For debugging purposes only.

Examples

The following example show sample output for the **show ip bgp attribute-entries** command.

```
device> show ipv6 bgp attribute-entries

Total number of BGP Attribute Entries: 378
1       Next Hop  :::                MED :1              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   :(65002) 65001 4355 2548 3561 5400 6669 5548
        Address: 0x27a4cdb0  Hash:877 (0x03000000) Reference Counts: 2:0:2
…
```

show ipv6 bgp config

Displays active BGP4+ configuration information.

Syntax

show ipv6 bgp config

Modes

User EXEC mode

Examples

This example displays the active BGP4+ configuration information contained in the running configuration without displaying the entire running configuration.

```
device> show ipv6 bgp config

Current BGP configuration:
router bgp
 local-as 1000
 neighbor peer_group1 peer-group
 neighbor 2001:db8:e0ff:783a::3 remote-as 1001
 neighbor 2001:db8:edd3:8389::1 remote-as 1002
 neighbor 2001:db8:80::23 peer-group peer_group1
 neighbor 2001:db8:80::23 remote-as 1003
 address-family ipv6 unicast
 no neighbor 2001:db8:e0ff:783a::3 activate
 no neighbor 2001:db8:edd3:8389::1 activate
 no neighbor 2001:db8:80::23 activate
 exit-address-family

 address-family vpnv4
 exit-address-family

 address-family l2vpn
 network 2001:db8::/32
 neighbor peer_group1 activate
 neighbor 2001:db8:edd3:8389::1 activate
 exit-address-family

end
```

show ipv6 bgp dampened-paths

Displays all BGP4+ dampened routes.

Syntax

show ipv6 bgp dampened-paths

Modes

User EXEC mode

Command Output

The **show ip bgp dampened-paths** command displays the following information:

Output field	Description
Status codes	A list of the characters the display uses to indicate the path's status. The status code appears in the left column of the display, to the left of each route. The status codes are described in the command's output. The status column displays a "d" for each dampened route.
Network	The destination network of the route.
From	The IPv6 address of the advertising peer.
Flaps	The number of times the path has flapped.
Since	The amount of time (in hh:mm:ss) since the first flap of this route.
Reuse	The amount of time (in hh:mm:ss) after which the path is available again.
Path	The AS path of the route.

Examples

The following example displays BGP4+ paths that have been dampened (suppressed) by route flap dampening.

```
device> show ipv6 bgp dampened-paths

Status Code >:best d:damped h:history *:valid
    Network               From                   Flaps     Since     Reuse     Path
*d     2001:db8:8::/45     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:1::/48     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:4::/46     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:2::/47     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:0:8000::/49     2001:db8:1::1     1     0 :1 :14     0 :2 :20     100 1002 1000
*d     2001:db8:17::/64    2001:db8:1::1     1     0 :1 :18     0 :2 :20     100
```

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*]

Parameters

detail

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 IPv6 prefix list. The name must be between 1 and 32 ASCII characters in length.

name

Name of an AS-path ACL or prefix list.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp filtered-routes** command displays the following information:

Output field	Description
Number of BGP4+ Routes matching display condition	The number of routes that matched the display parameters you entered. This is the number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the left column of the display, to the left of each route. The status codes are described in the command's output. The status column displays an "IF" for each filtered route.
Prefix	The network address and prefix.
Next Hop	The next-hop router for reaching the network from the device.
MED	The value of the route's MED attribute. If the route does not have a metric, this field is blank.

Output field	Description
LocPrf	The degree of preference for this route relative to other routes in the local AS. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The route's status, which can be one or more of the following: • A - AGGREGATE - The route is an aggregate route for multiple networks. • B - BEST - BGP4+ has determined that this is the optimal route to the destination. • b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes). • C - CONFED_EBGP - The route was learned from a neighbor in the same confederation and AS, but in a different sub-AS within the confederation. • D - DAMPED - This route has been dampened (by the route dampening feature), and is currently unusable. • E - EBGP - The route was learned through a in another AS. • H - HISTORY - Route dampening is configured for this route, and the route has a history of flapping and is unreachable now. • I - IBGP - The route was learned through a in the same AS. • L - LOCAL - The route originated on this device. • M - MULTIPATH - BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with "B". NOTE If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table. • S - SUPPRESSED - This route was suppressed during aggregation and thus is not advertised to neighbors. • F - FILTERED - This route was filtered out by BGP4+ route policies on the device, but the device saved updates containing the filtered routes.

Examples

This example displays BGP4+ filtered routes.

```
device> show ipv6 bgp filtered-routes

Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
       Prefix             Next Hop        MED LocPrf     Weight Status
1      2001:db8:3000::/48 2001:db8::110       100        0        EF
         AS_PATH: 65001 4355 701 80
2      2001:db8:4000::/48 2001:db8::110       100        0        EF
         AS_PATH: 65001 4355 1
3      2001:db8:5000::/48 2001:db8::110       100        0        EF
         AS_PATH: 65001 4355 701 1 189
```

This example displays detailed information for BGP4+ filtered routes.

```
device> show ipv6 bgp filtered-routes detail

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
1     Prefix: 2001:db8:1::/64, Status: EF, Age: 0h0m10s
    NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
    LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
    AS_PATH: 100
2     Prefix: 2001:db8:18::/64, Status: EF, Age: 0h0m10s
    NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
    LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
    AS_PATH: 100
3     Prefix: 2001:db8:1::/64, Status: EF, Age: 0h0m10s
    NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
    LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
    AS_PATH: 100
4     Prefix: 2001:db8:1::/64, Status: EF, Age: 0h0m10s
    NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
    LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
    AS_PATH: 100
5     Prefix: 2001:db8:11::1/128, Status: EF, Age: 0h0m10s
    NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
    LOCAL_PREF: 100, MED: 0, ORIGIN: igp, Weight: 0
    AS_PATH: 100
6     Prefix: 2001:db8:17::/64, Status: EF, Age: 0h0m10s
    NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
    LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
    AS_PATH: 100
```

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-prefix**]

show ipv6 bgp flap-statistics as-path-filter *name*

show ipv6 bgp flap-statistics neighbor *ipv6-addr*

show ipv6 bgp flap-statistics regular-expression *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.

as-path-filter *name*
Specifies an AS-path filter.

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

User EXEC mode

Command Output

The **show ipv6 bgp flap-statistics** command displays the following information:

Output field	Description
Total number of flapping routes	The total number of routes in the device's BGP4+ route table that have changed state and thus have been marked as flapping routes.

Output field	Description
Status code	Indicates the dampening status of the route, which can be one of the following: • > - This is the best route among those in the BGP4+ route table to the route's destination. • d - This route is currently dampened, and thus unusable. • h - The route has a history of flapping and is unreachable now. • * - The route has a history of flapping but is currently usable.
Network	The destination network of the route.
From	The IPv6 address of the advertising peer.
Flaps	The number of flaps (state changes) the route has experienced.
Since	The amount of time (in hh:mm:ss) since the first flap of this route.
Reuse	The amount of time (in hh:mm:ss) after which the path is again available.
Path	The AS path of the route.

Examples

The following example displays route dampening statistics.

```
device> show ipv6 bgp flap-statistics

Total number of flapping routes: 14
    Status Code  >:best d:damped h:history *:valid
    Network          From           Flaps  Since    Reuse    Path
h>  2001:db8:2::/48    2001:db8:23::47  1    0 :0 :13 0 :0 :0  65001 4355 1 701
*>  2001:db8:34::/48   2001:db8:23::47  1    0 :1 :4  0 :0 :0  65001 4355 701 62
```

show ipv6 bgp neighbors

Displays configuration information and statistics for BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors

show ipv6 bgp neighbors *ipv6-addr*

show ipv6 bgp neighbors last-packet-with-error

show ipv6 bgp neighbors routes-summary

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

last-packet-with-error

Displays information about the last packet from a neighbor that contained an error.

routes-summary

Displays information about all route information received in UPDATE messages from BGP neighbors.

Modes

User EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Command Output

The **show ipv6 bgp neighbors** command displays the following information:

Output field	Description
IP Address	The IPv6 address of the neighbor.
AS	The AS in which the neighbor resides.
EBGP or IBGP	Whether the neighbor session is an IBGP session, an EBGP session, or a confederation EBGP session: • EBGP - The neighbor is in another AS. • EBGP_Confed - The neighbor is a member of another sub-AS in the same confederation. • IBGP - The neighbor is in the same AS.
RouterID	The neighbor's router ID.

Output field	Description
State	The state of the device's session with the neighbor. The states are from the perspective of the session, not the neighbor's perspective. The state values can be one of the following: • IDLE - The BGP4+ process is waiting to be started. Usually, enabling BGP4 or establishing a neighbor session starts the BGP4+ process. – A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • ADMND - The neighbor has been administratively shut down. – A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • CONNECT - BGP4+ is waiting for the connection process for the TCP neighbor session to be completed. • ACTIVE - BGP4+ is waiting for a TCP connection from the neighbor. **NOTE** If the state frequently changes between CONNECT and ACTIVE, there may be a problem with the TCP connection. • OPEN SENT - BGP4+ is waiting for an Open message from the neighbor. • OPEN CONFIRM - BGP4+4 has received an OPEN message from the neighbor and is now waiting for either a KEEPALIVE or NOTIFICATION message. If the device receives a KEEPALIVE message from the neighbor, the state changes to Established. If the message is a NOTIFICATION, the state changes to Idle. • ESTABLISHED - BGP4+ is ready to exchange UPDATE messages with the neighbor. – If there is more BGP data in the TCP receiver queue, a plus sign (+) is also displayed. **NOTE** If you display information for the neighbor using the **show ipv6 bgp neighbor***<ipv6-address>* command, the TCP receiver queue value will be greater than 0.
Time	The amount of time this session has been in its current state.
KeepAliveTime	The keep alive time, which specifies how often this device sends keep alive messages to the neighbor.
HoldTime	The hold time, which specifies how many seconds the device will wait for a KEEPALIVE or UPDATE message from a BGP4+ neighbor before deciding that the neighbor is dead.
RefreshCapability	Whether the device has received confirmation from the neighbor that the neighbor supports the dynamic refresh capability.
Messages Sent and Received	The number of messages this device has sent to and received from the neighbor. The display shows statistics for the following message types: • Open • Update • KeepAlive • Notification • Refresh-Req
Last Update Time	Lists the last time updates were sent and received for the following: • NLRIs • Withdraws
Last Connection Reset Reason	The reason the previous session with this neighbor ended. The reason can be one of the following: • No abnormal error has occurred. • Reasons described in the BGP specifications: – Message Header Error

Output field	Description
	– Connection Not Synchronized – Bad Message Length – Bad Message Type – OPEN Message Error – Unsupported Version Number – Bad Peer AS Number – Bad BGP Identifier – Unsupported Optional Parameter – Authentication Failure – Unacceptable Hold Time – Unsupported Capability – UPDATE Message Error – Malformed Attribute List – Unrecognized Well-known Attribute – Missing Well-known Attribute – Attribute Flags Error – Attribute Length Error – Invalid ORIGIN Attribute – Invalid NEXT_HOP Attribute – Optional Attribute Error – Invalid Network Field – Malformed AS_PATH – Hold Timer Expired – Finite State Machine Error – Rcv Notification
Last Connection Reset Reason (cont.)	• Reasons specific to the implementation: – Reset All Peer Sessions – User Reset Peer Session – Port State Down – Peer Removed – Peer Shutdown – Peer AS Number Change – Peer AS Confederation Change – TCP Connection KeepAlive Timeout – TCP Connection Closed by Remote – TCP Data Stream Error Detected
Notification Sent	If the device receives a NOTIFICATION message from the neighbor, the message contains an error code corresponding to one of the following errors. Some errors have subcodes that clarify the reason for the error. Where applicable, the subcode messages are listed underneath the error code messages. • Message Header Error – Connection Not Synchronized – Bad Message Length – Bad Message Type – Unspecified • Open Message Error – Unsupported Version – Bad Peer As – Bad BGP Identifier – Unsupported Optional Parameter – Authentication Failure – Unacceptable Hold Time – Unspecified • Update Message Error – Malformed Attribute List – Unrecognized Attribute – Missing Attribute – Attribute Flag Error

Output field	Description
	– Attribute Length Error – Invalid Origin Attribute – Invalid NextHop Attribute – Optional Attribute Error – Invalid Network Field – Malformed AS Path – Unspecified • Hold Timer Expired • Finite State Machine Error • Cease • Unspecified
Notification Received	See above.
Neighbor NLRI Negotiation	The state of the device's NLRI negotiation with the neighbor. The states can include the following: • Peer negotiated IPv6 unicast capability. • Peer configured for IPv6 unicast routes. • Peer negotiated IPv4 unicast capability. • Peer negotiated IPv4 multicast capability.
TCP Connection state	The state of the connection with the neighbor. The connection can have one of the following states: • LISTEN - Waiting for a connection request. • SYN-SENT - Waiting for a matching connection request after having sent a connection request. • SYN-RECEIVED - Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTABLISHED - Data can be sent and received over the connection. This is the normal operational state of the connection. • FIN-WAIT-1 - Waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent. • FIN-WAIT-2 - Waiting for a connection termination request from the remote TCP. • CLOSE-WAIT - Waiting for a connection termination request from the local user. • CLOSING - Waiting for a connection termination request acknowledgment from the remote TCP. • LAST-ACK - Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request). • TIME-WAIT - Waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request. • CLOSED - There is no connection state.
Byte Sent	The number of bytes sent.
Byte Received	The number of bytes received.
Local host	The IPv6 address of the device.
Local port	The TCP port the Brocade device is using for the BGP4+ TCP session with the neighbor.
Remote host	The IPv6 address of the neighbor.
Remote port	The TCP port the neighbor is using for the BGP4+ TCP session with the device.
ISentSeq	The initial send sequence number for the session.
SendNext	The next sequence number to be sent.
TotUnAck	The number of sequence numbers sent by the device that have not been acknowledged by the neighbor.

Output field	Description
TotSent	The number of sequence numbers sent to the neighbor.
ReTrans	The number of sequence numbers that the device retransmitted because they were not acknowledged.
UnAckSeq	The current acknowledged sequence number.
IRcvSeq	The initial receive sequence number for the session.
RcvNext	The next sequence number expected from the neighbor.
SendWnd	The size of the send window.
TotalRcv	The number of sequence numbers received from the neighbor.
DupliRcv	The number of duplicate sequence numbers received from the neighbor.
RcvWnd	The size of the receive window.
SendQue	The number of sequence numbers in the send queue.
RcvQue	The number of sequence numbers in the receive queue.
CngstWnd	The number of times the window has changed.

Examples

The following is sample output from the **show ipv6 bgp neighbors** command when no arguments or keywords are used.

```
device> show ipv6 bgp neighbors

Total number of BGP Neighbors: 1
    '+': Data in InQueue '>': Data in OutQueue '-': Clearing
    '*': Update Policy 'c': Group change 'p': Group change Pending
    'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1   IP Address: 78:2::2, AS: 100 (IBGP), RouterID: 0.0.0.0, VRF: default-vrf
    State: CONNECT, Time: 0h9m7s, KeepAliveTime: 60, HoldTime: 180
    Minimal Route Advertisement Interval: 0 seconds
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 0       0       0         0            0
       Received: 0       0       0         0            0
    Last Connection Reset Reason:Unknown
    Notification Sent:     Unspecified
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer configured for IPV6 unicast  Routes
    Neighbor ipv6 MPLS Label Capability Negotiation:
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
       ID: 2, Use Count: 2
    BFD:Disabled
Error: TCP status not available
```

The following is sample output from the **show ipv6 bgp neighbors** command when an IPv6 address is specified.

```
device> show ipv6 bgp neighbors 2001:db8::110

1   IP Address: 2001:db8::110, AS: 65002 (EBGP), RouterID: 10.1.1.1
    State: ESTABLISHED, Time: 5d20h38m54s, KeepAliveTime: 60, HoldTime: 180
       RefreshCapability: Received
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 1       2       8012      0            0
       Received: 1       0       7880      0            0
    Last Update Time: NLRI       Withdraw          NLRI       Withdraw
                  Tx: ---        ---           Rx: ---        ---
    Last Connection Reset Reason:Unknown
    Notification Sent:     Unspecified
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer Negotiated IPV6 unicast  capability
      Peer configured for IPV6 unicast  Routes
    TCP Connection state: ESTABLISHED
       Byte Sent:   152411, Received: 149765
       Local host:  2001:db8::106, Local  Port: 8222
       Remote host: 2001:db8::110, Remote Port: 179
       ISentSeq:  740437769  SendNext:  740590181  TotUnAck:          0
       TotSent:      152412  ReTrans:           0  UnAckSeq:  740590181
       IRcvSeq:   242365900  RcvNext:   242515666  SendWnd:       16384
       TotalRcv:     149766  DupliRcv:          0  RcvWnd:        16384
       SendQue:           0  RcvQue:            0  CngstWnd:       1440
…
```

History

The following example displays information about the last error packet from any neighbor of the device.

```
device> show ipv6 bgp neighbors last-packet-with-error

Total number of BGP Neighbors: 266
No received packet with error logged for any neighbor
```

Release version	Command history
5.9.00	The command was modified. Description codes were added to display output.
6.0.0	This command was modified to include BGP add path configuration status.

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*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

detail

Specifies detailed information.

mask-bits

Number of mask bits in CIDR notation.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp neighbor advertised-routes** command displays the following information:

Output field	Description
Number of BGP4+ Routes advertised to specified neighbor (appears only in display for all routes)	The number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The advertised route's prefix.
Next Hop	The next-hop for reaching the advertised route from the device.
MED	The value of the advertised route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the advertised route relative to other routes in the local autonomous system. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference range is 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The advertised route's status, which can be one or more of the following: • A - AGGREGATE. The route is an aggregate route for multiple networks. • B - BEST. BGP4+ has determined that this is the optimal route to the destination. • b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device

Output field	Description
	received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes). • E - EBGP. The route was learned through a in another AS. • I - IBGP. The route was learned through a in the same AS. • L - LOCAL. The route originated on this device.
AS-PATH	The AS-path information for the route.

Examples

This example displays the routes the device has advertised to a specified neighbor.

```
device# show ipv6 bgp neighbor 2001:db8::110 advertised-routes

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop  MED LocPrf   Weight Status
1      2001:db8:1234::/48 ::        1            32768  BL
         AS_PATH:
2      2001:db8:2002::/48 ::        1            32768  BL
         AS_PATH:
```

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**

Parameters

ipv6-addr

IPv4 address of a neighbor in dotted-decimal notation.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp neighbor flap-statistics** command displays the following information:

Output field	Description
Total number of flapping routes	The total number of routes in the neighbor's BGP4+ route table that have changed state and thus have been marked as flapping routes.
Status code	Indicates the status of the route, which can be one of the following: • > - This is the best route among those in the neighbor's BGP4+ route table to the route's destination. • d - This route is currently dampened, and thus unusable. • h - The route has a history of flapping and is unreachable now. • * - The route has a history of flapping but is currently usable.
Network	The destination network of the route.
From	The IPv6 address of the advertising peer.
Flaps	The number of flaps (state changes) the route has experienced.
Since	The amount of time (in hh:mm:ss) since the first flap of this route.
Reuse	The amount of time (in hh:mm:ss) after which the path is again available.
Path	The AS path of the route.

Examples

This example displays route flap dampening statistics for a specified BGP4+ neighbor.

```
device> show ipv6 bgp neighbor 2001:db8::110 flap-statistics

Total number of flapping routes: 14
    Status Code  >:best d:damped h:history *:valid
    Network            From            Flaps Since    Reuse    Path
h>  2001:db8:2::/48    10.90.213.77    1     0 :0 :13 0 :0 :0  65001 4355 1 701
*>  2001:db8:34::/48   10.90.213.77    1     0 :1 :4  0 :0 :0  65001 4355 701 62
```

show ipv6 bgp neighbors last-packet-with-error

Displays the last packets with an error from BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **last-packet-with-error** [**decode**]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

decode

Decodes the last packet that contained an error from any of a device's neighbors.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp neighbor last-packet-with-error** command displays the following information:

Output field	Description
Total number of BGP Neighbors	The total number of configured neighbors for a device.
Last error	The error packet's contents decoded in a human-readable format or notification that no packets with an error were received.

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** { **extended-community** | **prefix-filter** }

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

extended-community

Displays the results for ORFs that use the BGP Extended Community Attribute.

prefix-filter

Displays the results for ORFs that are prefix-based.

Modes

User EXEC mode

Examples

This example displays sample output for the **show ipv6 bgp neighbors received** command when the **prefix-filter** keyword is used.

```
device> show ipv6 bgp neighbor 2001:db8::110 received prefix-filter

ip prefix-list 2001:db8::110: 4 entries
     seq 5 permit 2001:db8:3::45/16 ge 18 le 28
     seq 10 permit 2001:db8::4::88/24
     seq 15 permit 2001:db8:5::37/8 le 32
     seq 20 permit 2001:db8:6::83/16 ge 18
```

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 *iipv6-addr* **received-routes** [**detail**]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

detail

Displays detailed route information.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp neighbor received-routes** command displays the following information:

Output field	Description
Number of BGP4+ Routes received from a neighbor	The number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The received route's prefix.
Next Hop	The IPv6 address of the next device that is used when forwarding a packet to the received route.
MED	The value of the route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the advertised route relative to other routes in the local autonomous system. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The advertised route's status, which can be one or more of the following: A - AGGREGATE. The route is an aggregate route for multiple networks. B - BEST. BGP4+ has determined that this is the optimal route to the destination. b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes).

Output field	Description
	D - DAMPED. This route has been dampened (by the route dampening feature), and is currently unusable. E - EBGP. The route was learned through a in another AS. H - HISTORY. Route dampening is configured for this route, and the route has a history of flapping and is unreachable now. I - IBGP. The route was learned through a in the same autonomous system. L - LOCAL. The route originated on this device. M - MULTIPATH. BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with "B". NOTE If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table. S - SUPPRESSED. This route was suppressed during aggregation and thus is not advertised to neighbors. F - FILTERED. This route was filtered out by BGP4+ route policies on the device, but the saved updates containing the filtered routes.

Examples

The following example displays a summary of the route information received in route updates from neighbor 2001:db8::10.

```
device> show ipv6 bgp neighbor 2001:db8::10 received-routes
There are 4 received routes from neighbor 2001:db8::10
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
    Prefix    Next Hop    Metric    LocPrf    Weight    Status
1     2001:db8:2002::/64    2001:db8::10     0    100     0    BE
AS_PATH: 400
2     2001:db8:2003::/64    2001:db8::10     1    100     0    BE
AS_PATH: 400
3     2001:db8:2004::/64    2001:db8::10     1    100     0    BE
AS_PATH: 400
4     2001:db8:2005::/64    2001:db8::10     1    100     0    BE
AS_PATH: 400
```

The following example displays output for the **show ipv6 bgp neighbor received-routes** when the **details** keyword is used.

```
device> show ipv6 bgp neighbor 2001:db8:1::1 received-routes detail

There are 4 received routes from neighbor 2001:db8:1::1
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
1 Prefix: 2001:db8:1000:1::/64, Status: BI, Age: 0h17m25s
NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
AS_PATH:
Adj_RIB_out count: 1, Admin distance 200
2 Prefix: 2001:db8:1::/64, Status: I, Age: 0h17m25s
NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
AS_PATH:
3 Prefix: 2001:db8:11::1/128, Status: BI, Age: 0h17m25s
NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
LOCAL_PREF: 100, MED: 0, ORIGIN: igp, Weight: 0
AS_PATH:
Adj_RIB_out count: 1, Admin distance 200
4 Prefix: 2001:db8:17::/64, Status: BI, Age: 0h17m25s
NEXT_HOP: 2001:db8:1::1, Learned from Peer: 2001:db8:1::1 (100)
LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
AS_PATH:
Adj_RIB_out count: 1, Admin distance 200
```

show ipv6 bgp neighbors rib-out-routes

Displays information about the current BGP4+ Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **rib-out-routes** [**detail**] [*ipv6-addr* [**/** *mask*]]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

last-packet-with-error

Displays the last packet with an error.

routes-summary

Displays routes received, routes accepted, number of routes advertised by peer, and so on.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp neighbors rib-out-routes** command displays the following information:

Output field	Description
Number of RIB_out routes for a specified neighbor (appears only in display for all RIB routes)	The number of RIB routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The RIB route's prefix.
Next Hop	The next-hop router for reaching the route from the device.
MED	The value of the advertised route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the route relative to other routes in the local autonomous system. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The RIB route's status, which can be one or more of the following: • A - AGGREGATE. The route is an aggregate route for multiple networks. • B - BEST. BGP4+ has determined that this is the optimal route to the destination. • E - EBGP. The route was learned through a in another autonomous system. • I - IBGP. The route was learned through a in the same autonomous system.

Output field	Description
	• L - LOCAL. The route originated on this device.
AS-PATH	The AS-path information for the route.

Examples

The following example displays a summaryabout all RIB routes for neighbor 2001:db8::110.

```
device> show ipv6 bgp neighbor 2001:db8::110 rib-out-routes

       There are 2 RIB_out routes for neighbor 2001:db8::110
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop     Metric    LocPrf     Weight Status
1      2001:db8:1234::/48  ::           1         100        32768  BL
         AS_PATH:
2      2001:db8:2002::/48  ::           1         100        32768  BL
         AS_PATH:
```

The following example displays detailed information about all RIB routes for neighbor 2001:db8::110.

```
device> show ipv6 bgp neighbor 2001:db8::110 rib-out-routes detail

                    There are 2 RIB_out routes for neighbor 2001:db8::110
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
1       Prefix: 2001:db8:1234::/48,  Status: BL,  Age: 6d18h17m53s
         NEXT_HOP: ::,  Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 1,  ORIGIN: incomplete,  Weight: 32768
           AS_PATH:
            Adj_RIB_out count: 1,  Admin distance 190
2       Prefix: 2001:db8:2002::/48,  Status: BL,  Age: 6d18h21m8s
         NEXT_HOP: ::,  Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 1,  ORIGIN: incomplete,  Weight: 32768
           AS_PATH:

            Adj_RIB_out count: 1,  Admin distance 190
            Adj_RIB_out count: 1,  Admin distance 190
```

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**

show ipv6 bgp neighbors *ipv6-addr* **routes** { **best** | **not-installed-best** | **unreachable** }

show ipv6 bgp neighbors *ipv6-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** }

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 RIP, OSPF, or static route to the next hop.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp neighbors routes** command displays the following information:

Output field	Description
Number of accepted routes from a specified neighbor	The number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The route's prefix.
Next Hop	The next-hop router for reaching the route from the device.
MED	The value of the route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the route relative to other routes in the local autonomous system. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.

Output field	Description
Status	The route's status, which can be one or more of the following: • A - AGGREGATE. The route is an aggregate route for multiple networks. • B - BEST. BGP4+ has determined that this is the optimal route to the destination. • C - CONFED_EBGP. The route was learned from a neighbor in the same confederation and autonomous system, but in a different sub-AS within the confederation. • D - DAMPED. This route has been dampened (by the route dampening feature), and is currently unusable. • E - EBGP. The route was learned through a in another autonomous system. • H - HISTORY. Route dampening is configured for this route, and the route has a history of flapping and is unreachable now. • I - IBGP. The route was learned through a in the same autonomous system. • L - LOCAL. The route originated on this device. • M - MULTIPATH. BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with "B". NOTE If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table. • S - SUPPRESSED. This route was suppressed during aggregation and thus is not advertised to neighbors. • F - FILTERED. This route was filtered out by BGP4+ route policies on the device, but the saved updates containing the filtered routes.
AS-PATH	The AS-path information for the route.

Examples

The following example shows sample output for the **show ip bgp neighbors routes** command when the **best** keyword is used.

```
device> show ipv6 bgp neighbor 2001:db8::106 routes best

       There are 2 accepted routes from neighbor 2001:db8::106
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
       Prefix                  Next Hop        MED LocPrf     Weight Status
1      2001:db8:2002::/48      2001:db8::106   1      100        0      BE
         AS_PATH: 65001
2      2001:db8:2002:1234::/64 2001:db8::106   1      100        0      BE
         AS_PATH: 65001
```

The following example shows detailed sample output for the **show ip bgp neighbors routes** command when the **best** keyword is used.

```
device> show ipv6 bgp neighbor 2000:4::106 routes detail best

       There are 2 accepted routes from neighbor 2000:4::106
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED F:FILTERED
1       Prefix: 2001:db8::/32,  Status: BE,  Age: 18h48m56s
         NEXT_HOP: 2001:db8::106,  Learned from Peer: 2001:db8::106 (65001)
          LOCAL_PREF: 100,  MED: 1,  ORIGIN: incomplete,  Weight: 0
           AS_PATH: 65001
2       Prefix: 2001:db8:1234::/48,  Status: BE,  Age: 18h48m56s
         NEXT_HOP: 2001:db8::106,  Learned from Peer: 2001:db8::106 (65001)
          LOCAL_PREF: 100,  MED: 1,  ORIGIN: incomplete,  Weight: 0
           AS_PATH: 65001
```

show ipv6 bgp neighbors routes-summary

Displays route summary information for all neighbors or a specified neighbor.

Syntax

show ipv6 bgp neighbors *ipv6-addr* **routes-summary**

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp neighbor 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, RIPng, 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 RIPng, OSPFv3, or static IPv6 route to the next hop.
History Routes	The number of routes that are down but are being retained for route flap dampening purposes.
NLRIs Received in Update Message	The number of routes received in Network Layer Reachability (NLRI) format in UPDATE messages: • Withdraws - The number of withdrawn routes the device has received. • Replacements - The number of replacement routes the device has received.
NLRIs Discarded due to	Indicates the number of times the device discarded an NLRI for the neighbor due to the following reasons: • Maximum Prefix Limit - The device's configured maximum prefix amount had been reached. • AS Loop - An AS loop occurred. An AS loop occurs when the BGP4+ AS-path attribute contains the local AS number. • Invalid Nexthop Address - The next hop value was not acceptable.

Output field	Description
	• 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 displays routes summary information for neighbor 2001:db8::110.

```
device> show ipv6 bgp neighbor 2001:db8::110 routes-summary

1   IP Address: 2001:db8::110
Routes Accepted/Installed:0,  Filtered/Kept:0,  Filtered:0
   Routes Selected as BEST Routes:0
      BEST Routes not Installed in IP Forwarding Table:0
   Unreachable Routes (no IGP Route for NEXTHOP):0
   History Routes:0

NLRIs Received in Update Message:0,  Withdraws:0 (0),  Replacements:0
   NLRIs Discarded due to
      Maximum Prefix Limit:0, AS Loop:0
      Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
      Duplicated Originator_ID:0, Cluster_ID:0

Routes Advertised:2,  To be Sent:0,  To be Withdrawn:0
NLRIs Sent in Update Message:2,  Withdraws:0,  Replacements:0

Peer Out of Memory Count for:
   Receiving Update Messages:0, Accepting Routes(NLRI):0
   Attributes:0, Outbound Routes(RIB-out):0 Outbound Routes Holder:0
```

show ipv6 bgp nexthop

Displays information about BGP nexthops.

Syntax

show ipv6 bgp nexthop [*ipv6-address* | **reachable** | **unreachable**]

Parameters

ipv6-address
Specifies an IPv6 address.

reachable
Specifies reachable nexthops.

unreachable
Specifies unreachable nexthops.

Modes

User EXEC mode

show ipv6 bgp peer-group

Displays peer-group information.

Syntax

show ipv6 bgp peer-group *peer-group-name*

Parameters

peer-group-name

Specifies a peer group name.

Modes

User EXEC mode

Usage Guidelines

Only the parameters that have values different from their defaults are listed.

Examples

This example shows sample output from the **show ipv6 bgp peer-group** command.

```
device> show ipv6 bgp peer-group peer_group1

1   BGP peer-group is pg1, Remote AS: 65002
    Description: device group 1
       NextHopSelf: yes
      Address family : IPV4 Unicast
      Address family : IPV4 Multicast
      Address family : IPV6 Unicast
    Members:
       IP Address: 10.169.102.2
       IP Address: 10.169.100.2
       IP Address: 10.169.101.2
       IP Address: 10.169.103.2
       IP Address: 10.169.104.2
       IP Address: 10.169.105.2
       IP Address: 10.169.106.2
       IP Address: 10.169.107.2
       IP Address: 10.169.108.2
       IP Address: 10.169.109.2
       IP Address: 10.169.110.2
       IP Address: 10.169.111.2
       IP Address: 10.169.112.2
```

show ipv6 bgp routes

Displays statistics for the routes in the device's BGP4+ route table.

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**]

Parameters

num
Table entry at which the display starts. For example, if you want to list entries beginning with table entry 100, specify 100.

ipv6-address/prefix
Specifies an IPv6 address and prefix.

age *num*
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).

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.

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 *ipv6-addr*
Displays BGP4+ route information about selected BGP neighbors.

nexthop *ipv6-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 a prefix list.

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 BGP route table.

Modes

User EXEC mode

Command Output

The **show ipv6 bgp routes detail** command displays the following information:

Output field	Description
Number of BGP4+ Routes	The number of routes displayed by the command.
Status codes	A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.
Prefix	The route's prefix.
Next Hop	For normal IPv6 routes, next hop is the next hop IPv6 router to reach the destination. For the 6PE routes, next hop is the IPv4-mapped IPv6 address of the peer 6PE router.
Metric	The value of the route's MED attribute. If the route does not have a metric, this field is blank.
LocPrf	The degree of preference for the advertised route relative to other routes in the local AS. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.
Weight	The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.
Status	The route's status, which can be one or more of the following: • A - AGGREGATE. The route is an aggregate route for multiple networks. • B - BEST. BGP4+ has determined that this is the optimal route to the destination. • b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes). • C - CONFED_EBGP. The route was learned from a neighbor in the same confederation and AS, but in a different sub-AS within the confederation. • D - DAMPED. This route has been dampened (by the route dampening feature), and is currently unusable. • E - EBGP. The route was learned through a in another AS. • H - HISTORY. Route dampening is configured for this route, and the route has a history of flapping and is unreachable now.

Output field	Description
	• I - IBGP. The route was learned through a in the same AS. • L - LOCAL. The route originated on this. • M - MULTIPATH. BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with "B". NOTE If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table. • S - SUPPRESSED. This route was suppressed during aggregation and thus is not advertised to neighbors.
AS-PATH	The AS-path information for the route.

Examples

The following example shows sample output from the **show ipv6 bgp routes** command.

```
device> show ipv6 bgp routes

Total number of BGP Routes: 4
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop    MED    LocPrf    Weight Status
1          2001:db8:1::/64   2001:db8:1111::2     1      100      32768       BL

        AS_PATH:
2          2001:db8:2::/64   2001:db8::30.30.30.1    1      100      0           BI

        AS_PATH:
3          2001:db8:1111::/64 ::                  0      100      32768       BL

        AS_PATH:
4          2001:db8:2222::/64 2001:db8::30.30.30.1    0      100     0           BI

        AS_PATH:
```

The following example shows sample output from the **show ipv6 bgp routes** command when the **detail** keyword is used.

```
device> show ipv6 bgp route detail

Total number of BGP Routes: 4
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1 Prefix: 2001:db8:1::/64,  Status: BL,  Age: 0h1m14s
    NEXT_HOP: 2001:db8:1111::2, Learned from Peer: Local Router
    In-Label: 794624
    LOCAL_PREF: 100,  MED: 1,  ORIGIN: incomplete,  Weight: 32768
    AS_PATH:
    Adj_RIB_out count: 1,  Admin distance 1
2 Prefix: 2001:db8:2::/64,  Status: BI,  Age: 0h0m8s
    NEXT_HOP: 2001:db8::ffff:30:1, Metric: 1,  Learned from Peer: 10.30.30.1 (1)
    Out-Label: 794624
    LOCAL_PREF: 100,  MED: 1,  ORIGIN: incomplete,  Weight: 0
    AS_PATH:
3 Prefix: 2001:db8:1111::/64,  Status: BL,  Age: 0h2m26s
    NEXT_HOP: ::, Learned from Peer: Local Router
    In-Label: 794624
    LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 32768
    AS_PATH:
    Adj_RIB_out count: 1,  Admin distance 1
4 Prefix: 2001:db8:2222::/64,  Status: BI,  Age: 0h0m35s
    NEXT_HOP: 2001:db8::ffff:30:1, Metric: 1,  Learned from Peer: 10.30.30.1 (1)
    Out-Label: 794624
    LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
    AS_PATH:
```

History

Release version	Command history
6.0.0	Command output was modified to include details about BGP additional paths.

show ipv6 bgp routes community

Displays BGP4+ route information that is filtered by community and other options.

Syntax

show ipv6 bgp routes community { *num* | *aa:nn* | **internet** | **local-as** | **no-advertise** | **no-export** }

Parameters

community

Displays routes filtered by a variety of communities.

num

Specifies a community number n the range from 1 to 4294967200.

aa:nn

Specifies an autonomous system-community number.

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.

Modes

User EXEC mode

show ipv6 bgp summary

Displays summarized information about the status of all BGP4+ connections.

Syntax

show ipv6 bgp summary

Modes

User EXEC mode

Command Output

The **show ipv6 bgp summary** command displays the following information.

Output field	Description
Router ID	The device's router ID.
Local AS Number	The BGP4+ AS number in which the device resides.
Confederation Identifier	The autonomous system number of the confederation in which the device resides.
Confederation Peers	The numbers of the local autonomous systems contained in the confederation. This list matches the confederation peer list you configure on the device.
Maximum Number of Paths Supported for Load Sharing	The maximum number of route paths across which the device can balance traffic to the same destination. The feature is enabled by default but the default number of paths is 1. You can increase the number from 2 - 8 paths.
Number of Neighbors Configured	The number of BGP4+ neighbors configured on this device.
Number of Routes Installed	The number of BGP4+ routes in the device's BGP4+ route table.
Number of Routes Advertising to All Neighbors	The total of the RtSent and RtToSend columns for all neighbors.
Number of Attribute Entries Installed	The number of BGP4+ route-attribute entries in the route-attributes table.
Neighbor Address	The IPv6 addresses of this BGP4+ neighbors.
AS#	The autonomous system number.
State	The state of this neighbor session with each neighbor. The states are from this perspective of the session, not the neighbor's perspective. The state values can be one of the following for each: • IDLE - The BGP4+ process is waiting to be started. Usually, enabling BGP4+ or establishing a neighbor session starts the BGP4+ process. – A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • ADMND - The neighbor has been administratively shut down. – A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes. • CONNECT - BGP4+ is waiting for the connection process for the TCP neighbor session to be completed. • ACTIVE - BGP4+ is waiting for a TCP connection from the neighbor.

Output field	Description
	NOTE If the state frequently changes between CONNECT and ACTIVE, there may be a problem with the TCP connection. • OPEN SENT - BGP4+ is waiting for an Open message from the neighbor. • OPEN CONFIRM - BGP4+ has received an OPEN message from the neighbor and is now waiting for either a KEEPALIVE or NOTIFICATION message. If the receives a KEEPALIVE message from the neighbor, the state changes to Established. If the message is a NOTIFICATION, the state changes to Idle. • ESTABLISHED - BGP4+ is ready to exchange UPDATE packets with the neighbor. – If there is more BGP data in the TCP receiver queue, a plus sign (+) is also displayed. NOTE If you display information for the neighbor using the **show ipv6 bgp neighbor**<*ipv6-address*> command, the TCP receiver queue value will be greater than 0. **Operational States:** Additional information regarding the operational states of BGP described above may be added as described in the following: • **(+)** - is displayed if there is more BGP data in the TCP receiver queue. **Note** : If you display information for the neighbor using the **show ip bgp neighbor***ip-addr* command, the TCP receiver queue value will be greater than 0. • **(>)** - indicates that there is more BGP data in the outgoing queue. • **(-)** - indicates that the session has gone down and the software is clearing or removing routes. • **(*)** - indicates that the inbound or outbound policy is being updated for the peer. • (**c**) - indicates that the table entry is clearing. • (**p**) - indicates that the neighbor ribout group membership change is pending or in progress • **(s)** - indicates that the peer has negotiated restart, and the session is in a stale state. • **(r)** - indicates that the peer is restarting the BGP4 connection, through restart. • **(^)** - on the standby MP indicates that the peer is in the ESTABLISHED state and has received restart capability (in the primary MP). • **(<)** - indicates that the device is waiting to receive the "End of RIB" message the peer.
Time	The time that has passed since the state last changed.
Accepted	The number of routes received from the neighbor that this installed in the BGP4+ route table. Usually, this number is lower than the RoutesRcvd number. The difference indicates that this filtered out some of the routes received in the UPDATE messages.
Filtered	The routes or prefixes that have been filtered out. • If soft reconfiguration is enabled, this field shows how many routes were filtered out (not placed in the BGP4+ route table) but retained in memory. • If soft reconfiguration is not enabled, this field shows the number of BGP4+ routes that have been filtered out.
Sent	The number of BGP4+ routes that the has sent to the neighbor.
ToSend	The number of routes the has queued to send to this neighbor.

Examples

This example displays sample output from the **show ipv6 bgp summary** command.

```
device> show ipv6 bgp summary

  BGP4 Summary
  Router ID: 10.7.7.7   Local AS Number: 100
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 1, UP: 0
  Number of Routes Installed: 0
  Number of Routes Advertising to All Neighbors: 0 (0 entries)
  Number of Attribute Entries Installed: 0
  '+': Data in InQueue '>': Data in OutQueue '-': Clearing
  '*': Update Policy 'c': Group change 'p': Group change Pending
  'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting
  Neighbor Address    AS#      State   Time        Rt:Accepted Filtered Sent  ToSend
  10:2::2             100      CONN    0h 9m 0s    0           0        0     0
```

History

Release version	Command history
5.9.00	The command was modified. Description codes were added to display output.

show ipv6 bgp vrf

Displays entries in the BGP4+ routing table for a virtual routing and forwarding (VRF) instance.

Syntax

show ipv6 bgp vrf *vrf-name*

show ipv6 bgp vrf *vrf-name ipv6-prefix /prefix-length*

show ipv6 bgp vrf *vrf-name ipv6 address/ /mask* [**longer-prefixes**]

show ipv6 bgp vrf *vrf-name ipv6 address/* [*/mask*] [**longer-prefixes**]

show ipv6 bgp vrf *vrf-name* **attribute-entries**

show ipv6 bgp vrf *vrf-name* **dampened-paths**

show ipv6 bgp vrf *vrf-name* **filtered-routes** [**detail**] [*ipv6-prefix* { **/** */prefix-length* } [**longer-prefixes**]] | **as-path-access-list** *name*] | **prefix-list** *name*]

show ipv6 bgp vrf *vrf-name* **flap-statistics**

show ipv6 bgp vrf *vrf-name* **flap-statistics** *ipv6-addr* { **/** *mask* } [**longer-prefix**]

show ipv6 bgp vrf *vrf-name* **flap-statistics as-path-filter** *name*

show ipv6 bgp vrf *vrf-name* **flap-statistics neighbor** *ipv6-addr*

show ipv6 bgp vrf *vrf-name* **flap-statistics regular-expression** *name*

show ipv6 bgp vrf *vrf-name* **nexthop** [*ipv6-addr* | **reachable** | **unreachable**]

show ipv6 bgp vrf *vrf-name* **peer-group** *peer-group-name*

show ipv6 bgp vrf *vrf-name* **summary**

Parameters

vrf-name
Specifies the name of a VRF instance.

ipv6-prefix
Specifies an IPv6 network number.

/prefix-length
Specifies the length of the IPv6 prefix.

ipv6 address /mask
Specifies an IPv6 address and mask.

longer-prefixes
Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

attribute-entries
Specifies BGP4+ route-attribute entries that are stored in device memory.

dampened-paths
Specifies multiprotocol BGP (MBGP) paths that have been dampened by route-flap dampening.

filtered-routes
Specifies BGP4+ filtered routes that are received from a neighbor or peer group.

detail
Optionally displays detailed route information.

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 IPv6 prefix list. The name must be between 1 and 32 ASCII characters in length.

flap-statistics
Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

as-path-filter *name*
Specifies an AS-path filter.

neighbor
Displays flap statistics only for routes learned from the specified neighbor.

ipv6-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.

nexthop
Specifies the configured next hop.

reachable
Specifies reachable next hops.

unreachable
Specifies unreachable next hops.

peer-group *peer-group-name*
Specifies a peer group.

summary
Displays summarized information.

Modes

User EXEC mode

show ipv6 bgp vrf neighbors

Displays configuration information and statistics for BGP4+ neighbors of the device for a virtual routing and forwarding (VRF) instance.

Syntax

show ipv6 bgp vrf *vrf-name* **neighbors** [*ipv6-addr*]

show ipv6 bgp vrf *vrf-name* **neighbors last-packet-with-error**

show ipv6 bgp vrf *vrf-name* **neighbors routes-summary**

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **advertised-routes** [**detail**] [*ipv6 address /mask*]

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **flap-statistics**

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **last-packet-with-error** [**decode**]

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **received** [**prefix-filter**]

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **received-routes** [**detail**]

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **rib-out-routes** [**detail**] [*ipv6 address /mask*]

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **routes**

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **routes** { **best** | **not-installed-best** | **unreachable** }

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** }

show ipv6 bgp vrf *vrf-name* **neighbors** *ipv6-addr* **routes-summary**

Parameters

vrf-name
Specifies the name of a VRF instance.

neighbors
Specifies a neighbor.

ipv6-addr
IPv6 address of a neighbor in dotted-decimal notation.

last-packet-with-error
Displays the last packet with an error.

routes-summary
Displays routes received, routes accepted, number of routes advertised by peer, and so on.

advertised-routes
Specifies the routes that the device has advertised to the neighbor during the current BGP4+ session.

detail
Specifies detailed information.

iipv6 address /mask
Specifies an IPv6 address and mask.

flap-statistics
Specifies the route flap statistics for routes received from or sent to a BGP4+ neighbor.

last-packet-with-error
Specifies the last packet with an error.

decode
Decodes the last packet that contained an error from any of a device's neighbors.

received
Specifies Outbound Route Filters (ORFs) received from BGP4+ neighbors of the device.

prefix-filter
Displays the results for ORFs that are prefix-based.

received-routes
Specifies all route information received in route updates from BGP4+ neighbors of the device since the soft-reconfiguration feature was enabled.

rib-out-routes
Displays information about the current BGP4+ Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

routes
Displays a variety of route information received in UPDATE messages from BGP4+ neighbors.

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.

routes-summary
Displays all route information received in UPDATE messages from BGP4+ neighbors.

Modes

User EXEC mode

show ipv6 bgp vrf routes

Displays statistics for the routes in the BGP4+ route table of a device for a virtual routing and forwarding (VRF) instance.

Syntax

show ipv6 bgp vrf *vrf-name* **routes** [**detail**] [*num* | *ipv6-address/prefix* | **age** *num* | **as-path-access-list** *name* | **best** | **cidr-only** | **community-access-list** *name* | **community-reg-expression** *expression* | **local** | **neighbor** *ipv6-addr* | **nexthop** *ipv6-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**]

Parameters

vrf-name
Specifies the name of a VRF instance.

detail
Displays detailed information.

num
Table entry at which the display starts. For example, if you want to list entries beginning with table entry 100, specify 100.

ipv6-address/prefix
Specifies an IPv6 address and prefix.

age *num*
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).

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.

community-reg-expression *expression*
Displays BGP4+ route information for an ordered community list regular expression.

local
Displays BGP4+ route information about selected local routes.

neighbor *ipv6-addr*
Displays BGP4+ route information about selected BGP neighbors.

nexthop *ipv6-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 a prefix list.

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 BGP route table.

Modes

User EXEC mode

show ipv6 bgp vrf routes community

Displays BGP4+ route information that is filtered by community and other options.

Syntax

show ipv6 bgp routes community { *num* | *aa:nn* | **internet** | **local-as** | **no-advertise** | **no-export** }

Parameters

community

Displays routes filtered by a variety of communities.

num

Specifies a community number n the range from 1 to 4294967200.

aa:nn

Specifies an autonomous system-community number.

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.

Modes

User EXEC mode

show ipv6 dhcp-relay interface

Displays the IPv6 DHCP relay information for a specific interface.

Syntax

show ipv6 dhcp-relay interface *stack/slot/port*

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show ipv6 dhcp-relay interface** command displays the following information:

Output field	Description
DHCPv6 Relay Information for *interface interface-type port-num*	The DHCPv6 relay information for the specific interface.
Destination	The configured destination IPv6 address.
OutgoingInterface	The interface on which the packet will be relayed if the destination relay address is a link local or multicast address.
Options	The current information about the DHCPv6 relay options for the interface.
Interface-Id	The interface ID option indicating whether the option is used.
Client-mac-address	Displays if the client MAC address is used or not.

Examples

The following example displays the DHCPv6 relay information for an interface.

```
device# show ipv6 dhcp-relay interface ethernet 4/1
DHCPv6 Relay Information for interface eth 4/1:
Destinations:
 Destination                  OutgoingInterface
 2000::1                      NA
Options:
 Interface-Id: Yes     Remote-Id:Yes     Client-mac-address:Yes
Prefix Delegation Information:
 Current:0 Maximum:8000 AdminDistance:10
```

History

Release version	Command history
5.4	This command was introduced.
5.9	This command was modified.

show ipv6 dhcp-relay options

Displays information about the relay options available to the prefixed delegates for a specific interface.

Syntax

show ipv6 dhcp-relay options

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show ipv6 dhcp-relay options** command displays the following information:

Output field	Description
Interface	The interface name.
Interface-Id	The interface ID option. Yes indicates the option is used; No indicates the option is not used.
Remote-Id	The remote ID option. Yes indicates the option is used; No indicates the option is not used.
Client-mac-address	The client MAC address option. Yes or No indicates if the option is used or not.

Examples

The following example displays relay options information.

```
device# show ipv6 dhcp-relay options
DHCPv6 Relay Options Information:
Interface       Interface-Id     Remote-Id     Client-mac-address
eth 4/1         Yes              Yes           Yes
```

History

Release version	Command history
5.4	This command was introduced.
5.9	This command was modified.

show ipv6 interface tunnel

Displays the IP addresses and unicast and multicast traffic counters for the specified IPv6 IPsec tunnel. This command cannot be used on IPv4 IPsec tunnels.

Syntax

show ipv6 interface tunnel *num*

Parameters

num

Specifies the tunnel number.

Modes

User EXEC mode

Command Output

The **show interfaces tunnel** command displays the following information:

Output field	Description
Tunnel number	The number of the tunnel.
Tunnel source	The IP address of the interface that is configured as the source of the tunnel. IP packets are forwarded from this interface across the tunnel.
Tunnel destination	The IP address of the interface that is configured as the destination of the tunnel. IP packets forwarded from the tunnel source interface are received by this interface.
Tunnel mode	The specified tunnel mode for the tunnel. This indicates which version of IP (IPv6 or IPv4) has been enabled on the tunnel interface. NOTE The tunnel mode is always IPv6 when using this command (this command can only be used on IPv6 IPsec tunnels).
Port name	The specified name of the port. If a name was not specified, the output shows no port name.
Internet address	The IP address of the port. This is not the IP address of the tunnel source or destination.
Tunnel TOS	The value to write into the ToS byte in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 99, where 0 means a tunnel packet copies the ToS value from the packet being encapsulated (the passenger packet).
Tunnel TTL	The value to write into the TTL field in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 255, where 0 means a tunnel packet copies thevalue from the packet being encapsulated (the passenger packet). The default value is 255.
Tunnel MTU	This maximum size allowable for IP packets entering the tunnel. Packets that exceed the value you specify (or the default) are sent back to the source. The default value is 1480 bytes.
Tunnel vrf	
Forwarding vrf	
Tunnel protection profile	The name of the IPsec profile used to encapsulate and encrypt the IP packets being transmitted by the tunnel interface. A tunnel profile defines a set of encapsulation and encryption methods used to secure IP packets.

Output field	Description
Tunnel packet statistics	The following packet counts for **unicast** traffic on the tunnel: • **RxPkts:** The total number of IP packets received from the tunnel on the interface. • **TxPkts:** The total number of IP packets transmitted across the tunnel from the interface. • **RxBytes:** The total number of bytes received from the tunnel on the interface. (The total is for IP packets only.) • **TxBytes:** The total number of bytes transmitted across the tunnel from the interface. (The total is for IP packets only.)
Tunnel multicast packet statistics	The following packet counts for **multicast** traffic on the tunnel: • **RxMcPkts:** The total number of IP multicast packets received from the tunnel on the interface. • **TxMcPkts:** The total number of IP multicast packets transmitted across the tunnel from the interface.

Usage Guidelines

This command is restricted to showing data for IPv6 IPsec tunnels.

NOTE

If you want to view the same information for IPv4 IPsec tunnels, use the **show interfaces tunnel** command.

Examples

History

Release version	Command history
05.9.00	This command was introduced.

show ipv6 match-payload-len

Displays details about the current IPv6 payload length system configuration.

Syntax

show ipv6 match-payload-len [**interface ethernet** *slot /port*

Parameters

interface ethernet

Displays resources used for IP multicast snooping.

slot/port

Specifies the interface slot and port.

Modes

User EXEC mode.

Usage Guidelines

Command Output

The **show ipv6 match-payload-len** command displays the following information:

Output field	Description
Slot	Slot number
PPCR	PPCR number
Min-Payload-length	Minimum payload length
Max-Payload-length	Maximum payload length

Examples

This show command displays the configuration for all PPCR on which IP payload length range is configured.

```
device(config)#show ipv6 match-payload-len
IPv6 Match Payload Length Configuration
Slot        PPCR          Min-Payload-length              Max-Payload-length
1             1                   0                              1000
1             2                   700                            1000
2             2                   800                            800
3             1                   700                            1000
3             2                   700                            1000
```

This show command displays the configuration on PPCR of the interface.

```
device(config)#show ipv6 match-payload-len interface ethernet 1/5
IPv6 Match Payload Length Configuration
Slot        PPCR        Min-Payload-length            Max-Payload-length
1             2               0                             1000
```

History

Release version	Command history
6.0.00a	This command was introduced.

show ipv6 mld cluster-client group

Displays the MLD cluster groups.

Syntax

show ipv6 mld cluster-client group { *group-address* [**detail**] }

Parameters

group-address
: Specifies the MLD cluster group address in CIDR notation.

detail
: Displays detailed information.

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays the MLD cluster client group.

```
device# show ipv6 mld cluster-client group 123::3
Total 1 groups
------------------------------------------------------------------------------------------------------
Idx  Group Address                            Port   Intf   GrpCmpV Mode    Timer Refreshed MDUPReq Srcs
----+----------------------------------------+------+------+-------+-------+-----+---------+-------+----
   1 123::3                                  e1/7   v10       Ver1 exclude   253     Y     N   0
```

History

Release version	Command history
06.1.00	This command was introduced.

show ipv6 pim counter mct

Displays the MLD MDUP statistics.

Syntax

show ipv6 pim counter mct

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays the MLD MDUP statistics.

```
device# #show ipv6 pim counter mct
Multicast MCT Statistics for IPv6 (DN):
Messages assembled into the send buffer  : 0
Messages processed out of the recv buffer: 0
Segments sent successfully to TCP        : 0
Segments failed to be accepted by TCP    : 0
Segments assembed into the receive buffer: 0
Messages dropped because (size > 12000)   : 0
Messages dropped because it won't fit into available space in send buffer   : 0
Segments dropped because it won't fit into available space in receive buffer: 0
Received messages dropped because of cluster-id mismatch                    : 0
Received messages dropped because the peer was not recognized               : 0
Received messages dropped because cluster not active                        : 0
Received messages dropped because MCT VLAN unrecognized                     : 0
Received messages dropped because of bad message type                       : 0
Received messages dropped because of bad checksum                           : 0
Received bytes skipped because of sync or checksum errors                   : 0
PIM Hello Messages sent  : 0
PIM J/P Messages sent    : 0
PIM Assert Messages sent : 0
PIM Unknown not sent     : 0
PIM Hello Messages received     : 0
PIM J/P Messages received       : 0
PIM Assert Messages received   : 0
PIM Unknown received & dropped : 0
MLDv1 reports sent  : 0
MLDv2 reports sent    : 0
MLD leaves sent : 0
MLD queries sent : 0
MLD unknown not sent     : 0
MLDv1 reports received  : 0
MLDv2 reports received  : 0
MLD leaves received   : 0
MLD queries received   : 0
MLD unknown received & dropped : 0
```

History

Release version	Command history
06.1.00	This command was modified to add MDUP statistics for MLD packets.

show ipv6 pim global

Displays the global IPv6 PIM settings.

Syntax

show ipv6 pim global

Modes

User EXEC mode

Global configuration mode

Examples

The following example displays the global IPv6 PIM settings.

```
device# show ipv6 pim global
Global IPv6 PIM Settings
  Fast Convergence          : disabled
  Scaling Optimization      : disabled
  MCT Scaling Optimization  : enabled
  LAG Rebalance             : disabled
  ECMP Type                 : disabled
  NSR Status                : disabled
  Trunk OIF Optimization    : enabled
  Port OIF Optimization     : enabled
  Rate-limit pkt cpu     : 4000        Rate-limit pkt reg         : 1000
  Rate-limit first data  : 2000        Rate-limit reg             : 2000
  Rate-limit wrong intf  : 10000       Rate-limit above threshold : 1000
  Rate-limit ageout      : 60000
  Rate-limit Update KAT  : 1000
  PIM Rate update        : 1
  LP stats traversal time: 0
```

History

Release version	Command history
06.1.00	This command was modified to add the MCT Scaling Optimization setting status.

show ipv6 ospf

Displays OSPFv3 information.

Syntax

show ipv6 ospf

Modes

User EXEC mode

Examples

The following example displays sample output from the **show ipv6 ospf** command.

```
device> show ipv6 ospf

OSPFv3 Process number 0 with Router ID 0xc0a862d5(192.168.98.213)
 Running 0 days 2 hours 55 minutes 36 seconds
 Number of AS scoped LSAs is 4
 Sum of AS scoped LSAs Checksum is 18565
 External LSA Limit is 250000
 Database Overflow Interval is 10
 Database Overflow State is NOT OVERFLOWED
 Route calculation executed 15 times
 Pending outgoing LSA count 0
 Authentication key rollover interval 300 seconds
 Number of areas in this router is 3
 Router is operating as ABR
 Router is operating as ASBR, Redistribute: CONNECTED RIP
 High Priority Message Queue Full count: 0
 Graceful restart helper is enabled, strict lsa checking is disabled
 Nonstop Routing is disabled

device> show ipv6 ospf

OSPFv3 Process number 0 with Router ID 0x10010101(10.1.1.1)
    Running 0 days 0 hours 1 minutes 53 seconds
    Number of AS scoped LSAs is 3
    Sum of AS scoped LSAs Checksum is fabdd4de
 External LSA Limit is 250000
 Database Overflow Interval is 10
 Database Overflow State is NOT OVERFLOWED
 Route calculation executed 0 times
 Pending outgoing LSA count 0
 Authentication key rollover interval 30 seconds
    Authentication key add/remove interval 0 seconds
 Number of areas in this router is 3
 Router is operating as ABR
 Router is operating as ASBR, Redistribute: CONNECTED
 High Priority Message Queue Full count: 0
 BFD is disabled
```

show ipv6 ospf area

Displays the OSPFv3 area table in a specified format.

Syntax

show ipv6 ospf area [*A.B.C.D*] [*decimal*]

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format.

Modes

User EXEC mode

Command Output

The **show ipv6 ospf area** command displays the following information:

Output field	Description
Area	The area number.
Interface attached to this area	The device interfaces attached to the area.
Number of Area scoped LSAs is *N*	Number of LSAs (*N*) with a scope of the specified area.
SPF algorithm executed is *N*	The number of times (*N*) the OSPF Shortest Path First (SPF) algorithm is executed within the area.
SPF last updated	The interval in seconds that the SPF algorithm was last executed within the area.
Current SPF node count	The current number of SPF nodes in the area.
Router	Number of router LSAs in the area.
Network	Number of network LSAs in the area.
Indx	The row number of the entry in the routers's OSPF area table.
Statistics of Area	The number of the area whose statistics are displayed.
Maximum hop count to nodes.	The maximum number of hop counts to an SPF node within the area.

Examples

The following example shows sample output from the **show ipv6 ospf area** command when no arguments or keywords are used.

```
device> show ipv6 ospf area
Area 0:
  Interface attached to this area: loopback 2 ethe 3/2 tunnel 2
        Number of Area scoped LSAs is 6
        Statistics of Area 0:
            SPF algorithm executed 16 times
            SPF last updated: 335256 sec ago
            Current SPF node count: 3
                Router: 2 Network: 1
                Maximum of Hop count to nodes: 2
```

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*]

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*]

show ipv6 ospf database scope { **area** { *A.B.C.D* | *decimal* } | **as** | **link** }

show ipv6 ospf database summary

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.

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.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 ospf database** command displays the following information:

Output field	Description
Area ID	The OSPF area in which the device resides.
Type	Type of LSA. LSA types can be the following: • Rtr - Router LSAs (Type 1). • Net - Network LSAs (Type 2). • Inap - Inter-area prefix LSAs for ABRs (Type 3). • Inar - Inter-area router LSAs for ASBRs (Type 4). • Extn - AS external LSAs (Type 5). • Link - Link LSAs (Type 8). • Iap - Intra-area prefix LSAs (Type 9).
LS ID	The ID of LSA in Decimal.
Adv Rtr	The device that advertised the route.
Seq(Hex)	The sequence number of the LSA. The OSPF neighbor that sent the LSA stamps it with a sequence number to enable the device and other OSPF routers to determine which LSA for a given route is the most recent.
Age	The age of the LSA, in seconds.
Chksum	A checksum for the LSA packet. The checksum is based on all the fields in the packet except the age field. The device uses the checksum to verify that the packet is not corrupted.
Len	The length, in bytes, of the LSA.
Sync	Sync status with the slave management processor (MP).

The **show ipv6 ospf database extensive** command displays the following information:

Output field	Description
Router LSA (Type 1) (Rtr) Fields	
Capability Bits	A bit that indicates the capability of the device. The bit can be set to one of the following: B - The device is an area border router. E - The device is an AS boundary router. V - The device is a virtual link endpoint. W - The device is a wildcard multicast receiver.
Options	A 24-bit field that enables IPv6 OSPF routers to support the optional capabilities. When set, the following bits indicate the following: V6 - The device should be included in IPv6 routing calculations. E - The device floods AS-external-LSAs as described in RFC 2740. MC - The device forwards multicast packets as described in RFC 1586. N - The device handles type 7 LSAs as described in RFC 1584. R - The originator is an active router. DC -The device handles demand circuits.
Type	The type of interface. Possible types can be the following: Point-to-point - A point-to-point connection to another router. Transit - A connection to a transit network. Virtual link - A connection to a virtual link.
Metric	The cost of using this router interface for outbound traffic.
Interface ID	The ID assigned to the router interface.
Neighbor Interface ID	The interface ID that the neighboring router has been advertising in hello packets sent on the attached link.
Neighbor Router ID	The router ID (IPv4 address) of the neighboring router that advertised the route. (By default, the router ID is the IPv4 address configured on the lowest numbered loopback interface. If the device does not have a loopback interface, the default router ID is the lowest numbered IPv4 address configured on the device.)
Network LSA (Type 2) (Net) Fields	
Options	A 24-bit field that enables IPv6 OSPF routers to support the optional capabilities. When set, the following bits indicate the following: V6 - The device should be included in IPv6 routing calculations. E - The device floods AS-external-LSAs as described in RFC 2740. MC - The device forwards multicast packets as described in RFC 1586. N - The device handles type 7 LSAs as described in RFC 1584. R - The originator is an active router. DC -The device handles demand circuits.
Attached Router	The address of the neighboring router that advertised the route.
Inter-Area Prefix LSA (Type 3) (Inap) Fields	
Metric	The cost of the route.

Output field	Description
Prefix Options	An 8-bit field describing various capabilities associated with the prefix.
Prefix	The IPv6 prefix included in the LSA.
Inter-Area Router LSA (Type 4) (Inar) Fields	
Options	A 24-bit field that enables IPv6 OSPF routers to support the optional capabilities. When set, the following bits indicate the following: V6 - The device should be included in IPv6 routing calculations. E - The device floods AS-external-LSAs as described in RFC 2740. MC - The device forwards multicast packets as described in RFC 1586. N - The device handles type 7 LSAs as described in RFC 1584. R - The originator is an active router. DC -The device handles demand circuits.
Metric	The cost of the route.
Destination Router ID	The ID of the router described in the LSA.
AS External LSA (Type 5) (Extn) Fields	
Bits	The bit can be set to one of the following: • E - If bit E is set, a Type 2 external metric. If bit E is zero, a Type 1 external metric. • F - A forwarding address is included in the LSA. • T - An external route tag is included in the LSA.
Metric	The cost of this route, which depends on bit E.
Prefix Options	An 8-bit field describing various capabilities associated with the prefix.
Referenced LS Type	If non-zero, an LSA with this LS type is associated with the LSA.
Prefix	The IPv6 prefix included in the LSA.
Link LSA (Type 8) (Link) Fields	
Router Priority	The router priority of the interface attaching the originating router to the link.
Options	The set of options bits that the router would like set in the network LSA that will be originated for the link.
Link Local Address	The originating router's link-local interface address on the link.
Number of Prefix	The number of IPv6 address prefixes contained in the LSA.
Prefix Options	An 8-bit field of capabilities that serve as input to various routing calculations: • NU - The prefix is excluded from IPv6 unicast calculations. • LA - The prefix is an IPv6 interface address of the advertising router. • MC - The prefix is included in IPv6 multicast routing calculations. • P - NSSA area prefixes are readvertised at the NSSA area border.
Prefix	The IPv6 prefix included in the LSA.
Intra-Area Prefix LSAs (Type 9) (Iap) Fields	
Number of Prefix	The number of prefixes included in the LSA.

Output field	Description
Referenced LS Type, Referenced LS ID	Identifies the router-LSA or network-LSA with which the IPv6 address prefixes are associated.
Referenced Advertising Router	The address of the neighboring router that advertised the route.
Prefix Options	An 8-bit field describing various capabilities associated with the prefix.
Metric	The cost of using the advertised prefix.
Prefix	The IPv6 prefix included in the LSA.
Number of Prefix	The number of prefixes included in the LSA.

Examples

The following example shows sample output from the **show ipv6 ospf database** 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           Iap  0        10.1.1.1     80000001  3    343d  52    Yes
0           Iap  0        10.2.2.2     80000001  8    c61d  58    No
```

The following example shows sample output from the **show ipv6 ospf database** command when the **advr** keyword is used.

```
device> show ipv6 ospf database advr 10.4.4.4

LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix
Area ID     Type LSID    Adv Rtr     Seq(Hex)  Age  Cksum  Len
1           Iap     0      10.4.4.4    80000001  1085  99fa  44

   Number of Prefix: 1
             Referenced LS Type: Router
             Referenced LS ID: 0
             Referenced Advertising Router: 10.4.4.4
             Prefix Options: Metric: 1
             Prefix: 2001:db8:11::/64

LSA Key - Rtr:Router Net:Network Inap:InterPrefix Inar:InterRouter
          Extn:ASExternal Grp:GroupMembership Typ7:Type7 Link:Link
          Iap:IntraPrefix
Area ID      Type LSID    Adv Rtr     Seq(Hex)  Age  Cksum  Len
1            Typ7     1     10.4.4.4    80000001  394  a8a6   36

   Bits: N--
             Metric: 1
   Prefix Options:
             Referenced LSType: 0
             Prefix: 2001:db8:11::/64
```

The following example shows sample output from the **show ipv6 ospf database** command when the **as-external** keyword is used.

```
device> show ipv6 ospf database as-external

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
N/A             Extn 2          192.168.98.213  80000004 895  6e5e  44    Yes
     Bits: E--
     Metric: 0
     Prefix Options:
     Referenced LSType: 0
     Prefix: 5100:213:213:0:192:213:1:0/112
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
N/A             Extn 1          192.168.98.190  80001394 643  1cc9  28    Yes
     Bits: E--
     Metric: 1
     Prefix Options:
     Referenced LSType: 0
     Prefix: ::/0
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
N/A             Extn 2          192.168.98.71   80000258 132  a3ff  32    Yes
     Bits: E-T
     Metric: 1
     Prefix Options:
     Referenced LSType: 0
     Prefix: ::/0
     Tag: 1
```

The following example shows sample output from the **show ipv6 ospf database** command when the **extensive** keyword is used.

```
device> show ipv6 ospf database extensive

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 LS ID     Adv Rtr     Seq(Hex)  Age  Cksum  Len
0          Link 00000031  10.1.1.1    80000001  35   6db9   56
   Router Priority: 1
   Options: V6E---R--
   LinkLocal Address: fe80::1
   Number of Prefix: 1
   Prefix Options:
   Prefix: 2001:db8:3002::/64

Area ID   Type LS ID      Adv Rtr         Seq(Hex)  Age  Cksum  Len
0         Iap     00000159  10.223.223.223  800000ab  357  946b   56
   Number of Prefix: 2
   Referenced LS Type: Network
   Referenced LS ID: 00000159
   Referenced Advertising Router: 10.223.223.223
   Prefix Options: Metric: 0
   Prefix: 2001:db8:2000:4::/64
   Prefix Options: Metric: 0
   Prefix: 2001:db8:46a::/64

Area ID   Type LS ID      Adv Rtr         Seq(Hex)  Age  Cksum  Len
0         Rtr 00000039    10.223.223.223  800000b1  355   8f2d   40
   Capability Bits: --EOptions:
   V6E---R--
   Type: Transit Metric: 1
   Interface ID: 00000058 Neighbor Interface ID: 00000058
   Neighbor Router ID: 10.223.223.223

Area ID  Type LS ID     Adv Rtr         Seq(Hex) Age  Cksum  Len
0        Net     000001f4 10.223.223.223  800000ab 346  190a   32
   Options: V6E---R--
   Attached Router: 10.223.223.223
   Attached Router: 10.1.1.1

Area ID   Type LS ID     Adv Rtr         Seq(Hex) Age  Cksum  Len
N/A       Extn 000001df  10.223.223.223  800000af 368  0aa8   32
   Bits: E
   Metric: 00000001
   Prefix Options:
   Referenced LSType: 0
   Prefix: 2001:db8::/32

Area ID  Type LS ID     Adv Rtr      Seq(Hex) Age  Cksum  Len
1        Inap 0000011d  10.1.1.188   80000001 124  25de   36
   Metric: 2
   Prefix Options:
   Prefix: 2001:db8:2::/64

Area ID  Type  LS ID     Adv Rtr     Seq(Hex)  Age  Cksum  Len
0        Inar  0000005b  10.1.1.198  80000001  990  dbad   32
   Options: V6E---R--
   Metric: 1
   Destination Router ID:10.1.1.188
```

show ipv6 ospf interface

Displays interface information for all or specific OSPFv3-enabled interfaces.

Syntax

show ipv6 ospf interface [**brief**] [**ethernet** *slot/port*] [**loopback** *number*] [**tunnel** *number*] [**ve** *number*]

Parameters

brief

Displays brief summary about OSPFv3-enabled interfaces.

ethernet

Specifies an Ethernet interface

slot

Specifies a valid slot number.

port

Specifies a valid port number.

loopback

Specifies a loopback interface.

port-number

Specifies the port number for the loopback interface.

tunnel

Specifies a tunnel.

number

Specifies a tunnel number.

ve

Specifies a virtual Ethernet interface.

vlan_id

Specifies the port number for the VE interface.

Modes

User EXEC mode

Usage Guidelines

Use the **brief** keyword to limit the display to the following fields:

- Interface
- Number of Interfaces
- Area
- Status

- Type
- Cost
- State
- Nbrs(F/C)

Command Output

The **show ipv6 ospf interface** command displays the following information:

Output field	Description
Interface status	The status of the interface. Possible status includes the following: • Up. • Down.
Type	The type of OSPFv3 circuit running on the interface. Possible types include the following: • BROADCAST • POINT TO POINT UNKNOWN • POINT TO POINT
IPv6 Address	The IPv6 address assigned to the interface.
Instance ID	An identifier for an instance of OSPFv3.
Router ID	The IPv4 address of the device. By default, the router ID is the IPv4 address configured on the lowest numbered loopback interface. If the device does not have a loopback interface, the default router ID is the lowest numbered IPv4 address configured on the device.
Area ID	The IPv4 address or numerical value of the area in which the interface belongs.
Cost	The overhead required to send a packet through the interface.
default	Shows whether or not the default passive state is set.
State	The state of the interface. Possible states include the following: • DR - The interface is functioning as the Designated Router for OSPFv3. • BDR - The interface is functioning as the Backup Designated Router for OSPFv3. • Loopback - The interface is functioning as a loopback interface. • P2P - The interface is functioning as a point-to-point interface. • Passive - The interface is up but it does not take part in forming an adjacency. • Waiting - The interface is trying to determine the identity of the BDR for the network. • None - The interface does not take part in the OSPF interface state machine. • Down - The interface is unusable. No protocol traffic can be sent or received on such a interface. • DR other - The interface is a broadcast or NBMA network on which another router is selected to be the DR. • Active - The interface sends or receives all the OSPFv3 control packets, and forms the adjacency.

Output field	Description
Transmit delay	The amount of time, in seconds, it takes to transmit Link State Updates packets on the interface.
Priority	The priority used when selecting the DR and the BDR. If the priority is 0, the interface does not participate in the DR and BDR election.
Timer intervals	The interval, in seconds, of the hello-interval, dead-interval, and retransmit-interval timers.
DR	The router ID (IPv4 address) of the DR.
BDR	The router ID (IPv4 address) of the BDR.
Number of I/F scoped LSAs	The number of interface LSAs scoped for a specified area, AS, or link.
DR Election	The number of times the DR election occurred.
Delayed LSA Ack	The number of the times the interface sent a delayed LSA acknowledgement.
Neighbor Count	The number of neighbors to which the interface is connected.
Adjacent Neighbor Count	The number of neighbors with which the interface has formed an active adjacency.
Neighbor	The router ID (IPv4 address) of the neighbor. This field also identifies the neighbor as a DR or BDR, if appropriate.
Interface statistics	The following statistics are provided for the interface: • Unknown - The number of Unknown packets transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received Unknown packets. • Hello - The number of Hello packets transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received Hello packets. • DbDesc - The number of Database Description packets transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received Database Description packets. • LSReq - The number of link-state requests transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received link-state requests. • LSUpdate - The number of link-state updates transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received link-state requests. • LSAck - The number of link-state acknowledgements transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received link-state acknowledgements.

The **show ipv6 ospf interface brief** command displays the following information:

Output field	Description
Number of Interfaces	Number of OSPFv3-enabled interfaces.
Interface	The interface type, and the port number or number of the interface.
Area	The OSPF area configured on the interface.

Output field	Description
Status	The status of the link and the protocol. Possible status include the following: • Up. • Down.
Type	The type of OSPFv3 circuit running on the interface. Possible types include the following: • BCST- Broadcast interface type • P2P- Point-to-point interface type • UNK- The interface type is not known at this time
Cost	The overhead required to send a packet across an interface.
State	The state of the interface. Possible states include the following: • DR - The interface is functioning as the Designated Router for OSPFv3. • BDR - The interface is functioning as the Backup Designated Router for OSPFv3. • Loopback - The interface is functioning as a loopback interface. • P2P - The interface is functioning as a point-to-point interface. • Passive - The interface is up but it does not take part in forming an adjacency. • Waiting - The interface is trying to determine the identity of the BDR for the network. • None - The interface does not take part in the OSPF interface state machine. • Down - The interface is unusable. No protocol traffic can be sent or received on such a interface. • DR other - The interface is a broadcast or NBMA network on which another router is selected to be the DR.
Nbrs (F/C)	The number of adjacent neighbor routers. The number to the left of the "/" are the neighbor routers that are fully adjacent and the number to the right represents all adjacent neighbor routers.

Examples

This example show sample output from the **show ipv6 ospf interface** command when no arguments or keywords are used.

```
device> show ipv6 ospf interface
eth 1/3 is down, type BROADCAST
 Interface is disabled
eth 1/8 is up, type BROADCAST
 IPv6 Address:
  2001:db8:18:18:18::1/64
  2001:db8:18:18::/64
 Instance ID 255, Router ID 10.1.1.1
 Area ID 1, Cost 1
  State Active(default passive) DR, Transmit Delay 1 sec, Priority 1
Timer intervals :
  Hello 10, Hello Jitter 10 Dead 40, Retransmit 5
 Authentication: Enabled
  KeyRolloverTime(sec): Configured: 30 Current: 0
  KeyRolloverState: NotActive
  Outbound: SPI:121212, ESP, SHA1
   Key:12345678901234567890123456789012345678901234567890
  Inbound: SPI:121212, ESP, SHA1
   Key:12345678901234567890123456789012345678901234567890
 DR:10.2.2.2 BDR:10.1.1.1 Number of I/F scoped LSAs is 2
 DRElection: 1 times, DelayedLSAck: 83 times
 Neighbor Count = 1, Adjacent Neighbor Count= 1
  Neighbor:
   10.2.2.2 (DR)
 Statistics of interface eth 1/8:
  Type     tx    rx     tx-byte    rx-byte
  Unknown  0     0      0          0
  Hello    1415  1408   56592      56320
  DbDesc   3     3      804        804
  LSReq    1     1      28         28
  LSUpdate 193   121    15616      9720
  LSAck    85    109    4840       4924
  OSPF messages dropped,no authentication: 0
eth 2/2 is up, type POINT-TO-POINT
 IPv6 Address:
  2001:db8:22:22::1/64
  2001:db8:22:22::/64
  2001:db8:202:202::1/64
  2001:db8:202:202::/64
 Instance ID 0, Router ID 10.1.1.1
 Area ID 100, Cost 1
 State P2P, Transmit Delay 1 sec, Priority 1
 Timer intervals:
  Hello 10, Hello Jitter 10 Dead 40, Retransmit 5
 Authentication: Enabled
  KeyRolloverTime(sec): Configured: 30 Current: 0
  KeyRolloverState: NotActive
  Outbound: SPI:11022, ESP, SHA1
   Key:12345678901234567890123456789012345678901234567890
  Inbound: SPI:11022, ESP, SHA1
   Key:12345678901234567890123456789012345678901234567890
  DR:0.0.0.0 BDR:0.0.0.0 Number of I/F scoped LSAs is 2
  ....................................
```

This example shows sample output from the **show ipv6 ospf interface** command when the **brief** keyword is used.

```
device> show ipv6 ospf interface brief
Number of Interfaces is 3

Interface     Area     Status  Type  Cost  State    Nbrs(F/C)
eth 1/1       1        up      BCST  1     BDR      0/1
eth 2/1       1        up      BCST  1     DR       0/0
loopback 1    1        up      BCST  1     Loopback 0/0
```

History

Release version	Command history
5.9.00	The **Number of Interfaces** field was added to the **show ipv6 ospf interface brief** field displays.

show ipv6 ospf memory

Displays information about OSPFv3 memory usage.

Syntax

show ipv6 ospf memory

Modes

User EXEC mode

Command Output

The **show ipv6 ospf memory** command displays the following information:

Output field	Description
Total Static Memory Allocated	A summary of the amount of static memory allocated, in bytes, to OSPFv3.
Total Dynamic Memory Allocated	A summary of the amount of dynamic memory allocated, in bytes, to OSPFv3.
Memory Type	The type of memory used by OSPFv3. (This information is for use by Brocade technical support in case of a problem.)
Size	The size of a memory type.
Allocated	The amount of memory currently allocated to a memory type.
Max-alloc	The maximum amount of memory that was allocated to a memory type.
Alloc-Fails	The number of times an attempt to allocate memory to a memory type failed.

Examples

The following is sample output from the **show ipv6 ospf memory** command.

```
device> show ipv6 ospf memory

Total Static Memory Allocated : 5829 bytes
Total Dynamic Memory Allocated : 0 bytes
 Memory Type               Size     Allocated  Max-alloc   Alloc-Fails
 MTYPE_OSPF6_TOP           0          0          0          0
 MTYPE_OSPF6_LSA_HDR       0          0          0          0
 MTYPE_OSPF6_RMAP_COMPILED 0          0          0          0
 MTYPE_OSPF6_OTHER         0          0          0          0
 MTYPE_THREAD_MASTER       0          0          0          0
 MTYPE_OSPF6_AREA          0          0          0          0
 MTYPE_OSPF6_AREA_RANGE    0          0          0          0
 MTYPE_OSPF6_SUMMARY_ADDRE 0          0          0          0
 MTYPE_OSPF6_IF            0          0          0          0
 MTYPE_OSPF6_NEIGHBOR      0          0          0          0
 MTYPE_OSPF6_ROUTE_NODE    0          0          0          0
 MTYPE_OSPF6_ROUTE_INFO    0          0          0          0
 MTYPE_OSPF6_PREFIX        0          0          0          0
 MTYPE_OSPF6_LSA           0          0          0          0
 MTYPE_OSPF6_VERTEX        0          0          0          0
 MTYPE_OSPF6_SPFTREE       0          0          0          0
 MTYPE_OSPF6_NEXTHOP       0          0          0          0
 MTYPE_OSPF6_EXTERNAL_INFO 0          0          0          0
 MTYPE_THREAD              0          0          0          0
```

show ipv6 ospf neighbor

Displays OSPFv3 neighbor information.

Syntax

show ipv6 ospf neighbor [**detail** | **router-id** *A.B.C.D*]

Parameters

detail

Displays detailed neighbor information.

router-id *A.B.C.D*

Displays neighbor information for the specified router ID.

Modes

User EXEC mode

Command Output

The **show ip ospf neighbor** command displays the following information:

Output field	Description
Router ID	The IPv4 address of the neighbor. By default, the router ID is the IPv4 address configured on the lowest numbered loopback interface. If the device does not have a loopback interface, the default router ID is the lowest numbered IPv4 address configured on the device.
Pri	The OSPFv3 priority of the neighbor. The priority is used during election of the DR and BDR.
State	The state between the device and the neighbor. The state can be one of the following: • Down • Attempt • Init • 2-Way • ExStart • Exchange • Loading • Full
DR	The router ID (IPv4 address) of the DR.
BDR	The router ID (IPv4 address) of the BDR.
Interface [State]	The interface through which the router is connected to the neighbor. The state of the interface can be one of the following: • DR - The interface is functioning as the Designated Router for OSPFv3. • BDR - The interface is functioning as the Backup Designated Router for OSPFv3.

Output field	Description
	• Loopback - The interface is functioning as a loopback interface. • P2P - The interface is functioning as a point-to-point interface. • Passive - The interface is up but it does not take part in forming an adjacency. • Waiting - The interface is trying to determine the identity of the BDR for the network. • None - The interface does not take part in the OSPF interface state machine. • Down - The interface is unusable. No protocol traffic can be sent or received on such an interface. • DR other - The interface is a broadcast or NBMA network on which another router is selected to be the DR.

The **show ip ospf neighbor router-id** command displays the following information:

Output field	Description
Router ID	The IPv4 address of the neighbor. By default, the router ID is the IPv4 address configured on the lowest numbered loopback interface. If the device does not have a loopback interface, the default router ID is the lowest numbered IPv4 address configured on the device.
Pri	The OSPFv3 priority of the neighbor. The priority is used during election of the DR and BDR.
State	The state between the device and the neighbor. The state can be one of the following: • Down • Attempt • Init • 2-Way • ExStart • Exchange • Loading • Full
DR	The router ID (IPv4 address) of the DR.
BDR	The router ID (IPv4 address) of the BDR.
Interface [State]	The interface through which the router is connected to the neighbor. The state of the interface can be one of the following: • DR - The interface is functioning as the Designated Router for OSPFv3. • BDR - The interface is functioning as the Backup Designated Router for OSPFv3. • Loopback - The interface is functioning as a loopback interface. • P2P - The interface is functioning as a point-to-point interface. • Passive - The interface is up but it does not take part in forming an adjacency. • Waiting - The interface is trying to determine the identity of the BDR for the network.

Output field	Description
	• None - The interface does not take part in the OSPF interface state machine. • Down - The interface is unusable. No protocol traffic can be sent or received on such a interface. • DR other - The interface is a broadcast or NBMA network on which another router is selected to be the DR.
DbDesc bit	The Database Description packet, which includes 3 bits of information: • The first bit can be "i" or "-". "i" indicates the inet bit is set. "-" indicates the inet bit is not set. • The second bit can be "m" or "-". "m" indicates the more bit is set. "-" indicates the more bit is not set. • The third bit can be "m" or "s". An "m" indicates the master. An "s" indicates standby.
Index	The ID of the LSA from which the neighbor learned of the router.
DR Decision	The router ID (IPv4 address) of the neighbor's elected DR and BDR.
Last Received Db Desc	The content of the last database description received from the specified neighbor.
Number of LSAs in Db Desc retransmitting	The number of LSAs that need to be retransmitted to the specified neighbor.
Number of LSAs in Summary List	The number of LSAs in the neighbor's summary list.
Number of LSAs in Request List	The number of LSAs in the neighbor's request list.
Number of LSAs in Retransmit List	The number of LSAs in the neighbor's retransmit list.
Seqnum Mismatch	The number of times sequence number mismatches occurred.
BadLSReq	The number of times the neighbor received a bad link-state request from the device.
One way received	The number of times a hello packet, which does not mention the router, is received from the neighbor. This omission in the hello packet indicates that the communication with the neighbor is not bidirectional.
Inactivity Timer	The number of times that the neighbor's inactivity timer expired.
Db Desc Retransmission	The number of times sequence number mismatches occurred.
LSReqRetrans	The number of times the neighbor retransmitted link-state requests to the device.
LSUpdateRetrans	The number of times the neighbor retransmitted link-state updates to the device.
LSA Received	The number of times the neighbor received LSAs from the device.
LS Update Received	The number of times the neighbor received link-state updates from the device.

Examples

The following is sample output from the **show ipv6 ospf neighbor** command.

```
device> show ipv6 ospf neighbor

RouterID     Pri State    DR              BDR         Interface [State]
10.1.1.1     1 Full       10.223.223.223  10.1.1.1    ethe 3/2  [DR]
```

The following is sample output from the **show ipv6 ospf neighbor** command when the **router-id** keyword is sued.

```
device> show ipv6 ospf neighbor router-id 10.3.3.3
RouterID     Pri State    DR          BDR         Interface [State]
10.3.3.3     1 Full       10.3.3.3    10.1.1.1    ve 10     [BDR]
   DbDesc bit for this neighbor: --s
   Nbr Ifindex of this router: 1
   Nbr DRDecision: DR 10.3.3.3, BDR 10.1.1.1
   Last received DbDesc: opt:xxx ifmtu:0 bit:--s seqnum:0
   Number of LSAs in DbDesc retransmitting: 0
   Number of LSAs in SummaryList: 0
   Number of LSAs in RequestList: 0
   Number of LSAs in RetransList: 0
   SeqnumMismatch 0 times, BadLSReq 0 times
   OnewayReceived 0 times, InactivityTimer 0 times
   DbDescRetrans 0 times, LSReqRetrans 0 times
   LSUpdateRetrans 1 times
   LSAReceived 12 times, LSUpdateReceived 6 times
```

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*

Parameters

A.B.C.D:M

Specifies an IPv6 network prefix.

Modes

User EXEC mode

Command Output

The **show ipv6 ospf redistribute route** command displays the following information:

Output field	Description
ID	An ID for the redistributed route.
Prefix	The IPv6 routes redistributed into OSPFv3.
Protocol	The protocol from which the route is redistributed into OSPFv3. Redistributed protocols can be the following: • BGP - BGP4+. • RIP - RIPng. • IS-IS – IPv6 IS-IS. • Static - IPv6 static route table. • Connected - A directly connected network.
Metric Type	The metric type used for routes redistributed into OSPFv3. The metric type can be the following: • Type-1 - Specifies a small metric (2 bytes). • Type-2 - Specifies a big metric (3 bytes).
Metric	The value of the default redistribution metric, which is the OSPF cost of redistributing the route into OSPFv3.

Examples

The following is sample output from the **show ipv6 ospf redistribute route** command when no IPv6 network prefix is specified.

```
device> show ipv6 ospf redistribute route

Id     Prefix                          Protocol  Metric Type  Metric
snIpAsPathAccessListStringRegExpression
1      2001:db8::/32                   Static    Type-2       1
2      2001:db8:1234::/48              Static    Type-2       0
```

The following is sample output from the **show ipv6 ospf redistribute route** command when an IPv6 network prefix is specified.

```
device> show ipv6 ospf redistribute route 2001:db8::
Id     Prefix                          Protocol  Metric Type  Metric
1      2001:db8::/32                   Static    Type-2       1
```

show ipv6 ospf routes

Displays OSPFv3 routes.

Syntax

show ipv6 ospf routes *A.B.C.D:M*

Parameters

A.B.C.D:M

Specifies a destination IPv6 address.

Modes

User EXEC mode

Command Output

The **show ipv6 ospf routes** command displays the following information:

Output field	Description
Current Route Count (Displays with the entire OSPFv3 route table only)	The number of route entries currently in the OSPFv3 route table.
Intra/Inter/External (Type1/Type2) (Displays with the entire OSPFv3 route table only)	The breakdown of the current route entries into the following route types: • Inter - The number of routes that pass into another area. • Intra - The number of routes that are within the local area. • External1 - The number of type 1 external routes. • External2 - The number of type 2 external routes.
Equal-cost multi-path (Displays with the entire OSPFv3 route table only)	The number of equal-cost routes to the same destination in the OSPFv3 route table. If load sharing is enabled, the device equally distributes traffic among the routes.
Destination	The IPv6 prefixes of destination networks to which the device can forward IPv6 packets. "*IA" indicates the next router is an intra-area router.
Cost	The type 1 cost of this route.
E2 Cost	The type 2 cost of this route.
Tag	The route tag for this route.
Flags	Flags associated with this route.
Dis	Administrative Distance for this route.
Next-Hop Router	The IPv6 address of the next router a packet must traverse to reach a destination.
Outgoing Interface	The router interface through which a packet must traverse to reach the next-hop router.
Adv_Router	The IP address of the advertising router.

Examples

The following example displays the entire OSPFv3 route table for the device.

```
device> show ipv6 ospf routes

Current Route count: 4
    Intra: 4 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:db8:200:1::1/128      0        0         0           00000003 110
   Next_Hop_Router            Outgoing_Interface Adv_Router
   ::                         loopback 1         10.1.2.1
   Destination                Cost     E2Cost    Tag         Flags    Dis
IA 2001:db8:300:1::1/128      0        0         0           00000003 110
   Next_Hop_Router            Outgoing_Interface Adv_Router
   ::                         loopback 2         10.1.2.1
   Destination                Cost     E2Cost    Tag         Flags    Dis
IA 2001:db8:400:1::1/128      0        0         0           00000003 110
   Next_Hop_Router            Outgoing_Interface Adv_Router
   ::                         loopback 1         10.1.2.1
   Destination                Cost      E2Cost   Tag         Flags    Dis
IA 2001:db8:500:1::1/128      1         0        0           00000003 110
   Next_Hop_Router            Outgoing_Interface Adv_Router
   ::                         loopback 2         10.1.2.1
```

The following example displays route information for the destination prefix 2000::.

```
device> show ipv6 ospf routes 2000::
Destination                 Cost      E2Cost    Tag       Flags    Dis
IA 2000::/64                1         0         0         00000003 110
   Next_Hop_Router           Outgoing_Interface Adv_Router
   ::                          eth 1/1            10.1.1.1
```

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* }]

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.

Modes

User EXEC mode

Command Output

The **show ipv6 ospf spf node** command displays the following information:

Output field	Description
SPF node	Each SPF node is identified by its device ID (IPv4 address). If the node is a child node, it is additionally identified by an interface on which the node can be reached appended to the router ID in the format *router-id* :*interface-id* .
Cost	The cost of traversing the SPF node to reach the destination.
Hops	The number of hops needed to reach the parent SPF node.
Next Hops to Node	The IPv6 address of the next hop-router or the router interface through which to access the next-hop router.
Parent Nodes	The SPF node's parent nodes. A parent node is an SPF node at the highest level of the SPF tree, which is identified by its router ID.
Child Nodes	The SPF node's child nodes. A child node is an SPF node at a lower level of the SPF tree, which is identified by its router ID and interface on which the node can be reached.

The **show ipv6 ospf spf table** command displays the following information:

Output field	Description
Destination	The destination of a route, which is identified by the following: • "R", which indicates the destination is a router. "N", which indicates the destination is a network. • An SPF node's device ID (IPv4 address). If the node is a child node, it is additionally identified by an interface on which the node can be reached appended to the router ID in the format *router-id :interface-id* .
Bits	A bit that indicates the capability of the device. The bit can be set to one of the following: • B - The device is an area border router. • E - The device is an AS boundary router. • V - The device is a virtual link endpoint. • W - The device is a wildcard multicast receiver.
Options	A 24-bit field that enables IPv6 OSPF routers to support the optional capabilities. When set, the following bits indicate the following: V6 - The router should be included in IPv6 routing calculations. E - The router floods AS-external-LSAs as described in RFC 2740. MC - The router forwards multicast packets as described in RFC 1586. N - The router handles type 7 LSAs as described in RFC 1584. R - The originator is an active router. DC -The router handles demand circuits.
Cost	The cost of traversing the SPF node to reach the destination.
Next hop	The IPv6 address of the next hop-router.
Interface	The router interface through which to access the next-hop router.

Examples

The following example shows information about SPF nodes in area 0.

```
device> show ipv6 ospf spf node area 0

SPF node for Area 0
SPF node 10.223.223.223,  cost: 0,  hops: 0
 nexthops to node:
 parent nodes:
 child nodes: 10.223.223.223:88
SPF node 10.223.223.223:88,  cost: 1,  hops: 1
 nexthops to node:    :: ethe 3/2
 parent nodes: 10.223.223.223
 child nodes: 10.1.1.1:0
SPF node 10.1.1.1:0,  cost: 1,  hops: 2
 nexthops to node:    fe80::2e0:52ff:fe91:bb37 ethe 3/2
 parent nodes: 10.223.223.223:88
 child nodes:
```

The following example displays the SPF table for area 0.

```
device> show ipv6 ospf spf table area 0

SPF table for Area 0
 Destination         Bits Options  Cost Nexthop                 Interface
R 10.1.1.1           ---- V6E---R-   1  fe80::2e0:52ff:fe91:bb37 ethe 3/2
N 10.223.223.223[88] ---- V6E---R-   1  ::                        ethe 3/2
```

The following example displays the SPF tree for area 0.

```
device> show ipv6 ospf spf tree area 0

   SPF tree for Area 0
 +- 10.223.223.223 cost 0
     +- 10.223.223.223:88 cost 1
         +- 10.1.1.1:0 cost 1
```

show ipv6 ospf summary

Displays summary information for all OSPFv3 instances.

Syntax

show ipv6 ospf summary

Modes

User EXEC mode

Examples

```
device> show ipv6 ospf summary

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     5       2       1         12      2
```

show ipv6 ospf virtual-links

Displays information about all OSPFv3 virtual links or specified links.

Syntax

show ipv6 ospf virtual-links [**brief**]

Parameters

brief

Displays summary information.

Modes

User EXEC mode

Command Output

The **show ipv6 ospf virtual-links** command displays the following information:

Output field	Description
Index	An index number associated with the virtual link.
Transit Area ID	The ID of the shared area of two ABRs that serves as a connection point between the two routers.
Router ID	Router ID of the router at the other end of the virtual link (virtual neighbor).
Interface Address	The local address used to communicate with the virtual neighbor.
State	The state of the virtual link. Possible states include the following: • P2P - The link is functioning as a point-to-point interface. • DOWN - The link is down.

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-link

Transit Area ID  Router ID        Interface Address             State
 1       1        10.1.1.1         201:db8::2                    P2P
```

show ipv6 ospf virtual-neighbor

Displays information about OSPFv3 virtual neighbors.

Syntax

show ipv6 ospf virtual-neighbor [**brief**]

Parameters

brief

Displays summary information.

Modes

User EXEC mode

Command Output

The **show ipv6 ospf virtual-neighbor** command displays the following information:

Output field	Description
Index	An index number associated with the virtual neighbor.
Router ID	IPv4 address of the virtual neighbor.
Address	The IPv6 address to be used for communication with the virtual neighbor.
State	The state between the device and the virtual neighbor. The state can be one of the following: • Down • Attempt • Init • 2-Way • ExStart • Exchange • Loading • Full
Interface	The interface type.
Option	The bits set in the virtual-link hello or database descriptors.
QCount	The number of packets that are in the queue and ready for transmission. If the system is stable, this number should always be 0.
Timer	A timer that counts down until a hello packet should arrive. If "timers" elapses and a hello packet has not arrived, the VL neighbor is declared to be down.

Examples

The following is sample output from the **show ipv6 ospf virtual-neighbor** command when no arguments or keywords are used:

```
device> show ipv6 ospf virtual-neighbor

Index Router ID        Address                       State     Interface
1     10.14.14.14      2001:db8:44:44::4             Full      eth 1/8
                Option: 00-00-00    QCount: 0    Timer: 408
2     10.14.14.14      2001:db8:44:44::4             Full      tunnel 256
                Option: 00-00-00    QCount: 0    Timer: 43
```

show ipv6 vrrp

Displays information about IPv6 Virtual Router Redundancy Protocol (VRRP) sessions.

Syntax

show ipv6 vrrp [**brief**]

show ipv6 vrrp [**ethernet** *slot*/*port* | **ve** *num*]

show ipv6 vrrp [**statistics** [**ethernet** *slot*/*port* | **ve** *num*]]

show ipv6 vrrp [**ve** *num* [**vrid** *VRID*]]

show ipv6 vrrp [**vrid** *VRID* [**ethernet** *slot*/*port* | **ve** *num*]]

Parameters

brief

Displays summary information about the IPv6 VRRP session.

ethernet *slot port*

Displays IPv6 VRRP information only for the specified Ethernet port. A forward slash "/" must be entered between the *slot* and *port* variables.

ve *num*

Displays IPv6 VRRP information only for the specified virtual Ethernet port.

statistics

Displays statistical information about the IPv6 VRRP session.

vrid *VRID*

Displays IPv6 VRRP information only for the specified virtual router ID (VRID).

Modes

User EXEC mode

Usage Guidelines

This command can be entered in any mode. This command supports IPv6 VRRP; to display information about VRRP Extended (VRRP-E) sessions, use the **show ipv6 vrrp-extended** command.

Command Output

The following is a partial list of output field descriptions for the **show ipv6 vrrp** command.

Output field	Description
Total number of VRRP routers defined	The total number of virtual routers configured and currently running on this Brocade device. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers.

Output field	Description
Interface	The interface on which VRRP is configured. If VRRP is configured on multiple interfaces, information for each interface is listed separately.
VRID	The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row.
state	This Brocade device's VRRP state for the virtual router. The state can be one of the following: • init—The virtual router is not enabled (activated). If the state remains init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other. If the state is init and the mode is incomplete, make sure you have specified the IP address for the virtual router. • backup—This Brocade device is a backup for the virtual router. • master—This Brocade device is the master for the virtual router.
current priority	The current VRRP priority of this Brocade device for the virtual router.
preempt-mode	Whether the backup preempt mode is enabled. If the backup preempt mode is enabled, this field contains a "true." If the mode is disabled, this field is blank.

Examples

The following example displays IPv6 VRRP session information in detail.

```
device(config)# show ipv6 vrrp

Total number of VRRP routers defined: 1
Interface 1/3
----------------
auth-type no authentication
VRID 13 (index 2)
interface 1/3
state master
administrative-status enabled
version v3
mode non-owner(backup)
virtual mac 0000.5e00.0217
priority 100
current priority 100
track-priority 1
hello-interval 1000 ms
backup hello-interval 60000 ms
advertise backup disabled
dead-interval 3000 ms
preempt-mode true
ipv6-address 3013::1
next hello sent in 700 ms
short-path-forwarding disabled
```

The following example displays IPv6 VRRP statistical information.

```
device# show ipv6 vrrp statistics

Global IPv6 VRRP statistics
-------------------------------
- received vrrp packets with checksum errors = 0
- received vrrp packets with invalid version number = 0
- received vrrp packets with unknown or inactive vrid = 0
Interface 1/3
----------------
VRID 13
- number of transitions to backup state = 1
- number of transitions to master state = 1
- total number of vrrp packets received = 0
. received backup advertisements = 19
. received packets with zero priority = 0
. received packets with invalid type = 0
. received packets with invalid authentication type = 0
. received packets with authentication type mismatch = 0
. received packets with authentication failures = 0
. received packets dropped by owner = 0
. received packets with ttl errors = 0
. received packets with ipv6 address mismatch = 0
. received packets with advertisement interval mismatch = 0
. received packets with invalid length = 0
- total number of vrrp packets sent = 1175
. sent backup advertisements = 0
. sent packets with zero priority = 0
- received neighbor solicitation packets dropped = 0
- received proxy neighbor solicitation packets dropped = 0
- received ipv6 packets dropped = 0
```

The following example displays IPv6 VRRP configuration information about VRID 1.

```
device# show ipv6 vrrp vrid 1

Interface 1/1
----------------
auth-type no authentication
VRID 1 (index 1)
interface 1/1
state master
administrative-status enabled
version v3
mode non-owner(backup)
virtual mac dddd.eeee.ffff (configured)
priority 100
current priority 100
track-priority 1
hello-interval 1000 ms
backup hello-interval 60000 ms
advertise backup disabled
dead-interval 3600 ms
preempt-mode true
ipv6 address 10:20:1::100
next hello sent in 400 ms
```

The following example displays an auto-generated IPv6 virtual link-local address used in the VRRPv3 VRID 1 instance.

NOTE

This example is applicable only to the auto-generation of an IPv6 virtual link-local address.

```
device# show ipv6 vrrp vrid 1

VRID 1 (index 1)
 interface 1/1
 state master
 administrative-status enabled
 version v3
 mode owner
 virtual mac 0000.5e00.0101
 virtual link-local fe80::200:5eff:fe00:201
 priority 255
 current priority 255
 track-priority 2
 hello-interval 1000 ms
 backup hello-interval 60000 ms
 number of configured virtual address 2
 ipv6-address 1:2:45::2
 ipv6-address 1:2:46::2
 next hello sent in 300 ms
 Track MCT-VPLS-State: Disable
```

History

Release version	Command history
5.9.00	This command was modified to display an auto-generated IPv6 virtual link-local address.

show ipv6 vrrp-extended

Displays information about IPv6 Virtual Router Redundancy Protocol Extended (VRRP-E) sessions.

Syntax

show ipv6 vrrp-extended [**brief**]

show ipv6 vrrp-extended [**ethernet** *slot*/*port* | **ve** *num*]

show ipv6 vrrp-extended [**statistics** [**ethernet** *slot*/*port* | **ve** *num*]]

show ipv6 vrrp-extended [**ve** *num* [**vrid** *VRID*]]

show ipv6 vrrp-extended [**vrid** *VRID* [**ethernet** *slot*/*port* | **ve** *num*]]

Parameters

brief
Displays summary information about the IPv6 VRRP-E session.

ethernet *slot port*
Displays IPv6 VRRP-E information only for the specified port.

statistics
Displays statistical information about the IPv6 VRRP-E session.

ve *num*
Displays IPv6 VRRP-E information only for the specified virtual Ethernet port.

vrid *VRID*
Displays IPv4 VRRP-E information only for the specified virtual-group ID.

Modes

User EXEC mode

Usage Guidelines

Use this command to display information about IPv6 VRRP-E sessions, either in summary or full-detail format. You can also specify a virtual group or interface for which to display output.

This command supports IPv6 VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Command Output

The **show ipv6 vrrp-extended** command displays the following information:

Output field	Description
Total number of VRRP-E routers defined	The total number of virtual routers configured on this Brocade device.

Output field	Description
	NOTE The total applies only to the protocol the Brocade device is running. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers.
Interface	The interface on which VRRP-E is configured. If VRRP-E is configured on multiple interfaces, information for each interface is listed separately.
VRID	The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row.
Current Priority	The current VRRP-E priority of this Brocade device for the virtual router.
Flags	Whether the backup preempt mode is enabled. If the backup preempt mode is enabled, this field contains a "P". If the mode is disabled, this field is blank. • P:Preempt 2:V2 3:V3 • 2: implies VRRP Version2 • 3: implies VRRP Version3
Short-Path-Fwd	This Brocade device's VRRP state for the virtual router. The state can be one of the following: • Init—The virtual router is not enabled (activated). If the state remains Init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other. NOTE If the state is Init and the mode is incomplete, make sure you have specified the IP address for the virtual router. • Backup—This Brocade device is a backup for the virtual router. • Master—This Brocade device is the master for the virtual router.
Master IP Address	The IPv6 address of the router interface that is currently the Master for the virtual router.
Backup IP Address	The IPv6 addresses of the router interfaces that are currently backups for the virtual router.
Virtual IP Address	The virtual IPv6 address that is being backed up by the virtual router.

Examples

The following example displays summary information for an IPv6 VRRP-E session.

```
device(config)# show ipv6 vrrp-extended brief

Total number of VRRP routers defined: 1
Flags Codes - P:Preempt 2:V2 3:V3 S:Short-Path-Fwd
Intf   VRID  CurrPrio Flags State   Master-IPv6 Backup-IPv6 Virtual-IPv6
                                    Address     Address     Address
------------------------------------------------------------------------
1/3    2     100      P3-   Master  Local       3013::2     3013::99
```

The following example displays detailed IPv6 VRRP-E configuration information about VRID 1.

```
device# show ipv6 vrrp-extended vrid 1

Interface 1/1/1
----------------
auth-type md5-authentication
VRID 1 (index 1)
interface 1/1/1
state master
administrative-status enabled
mode non-owner(backup)
virtual mac dddd.eeee.ffff (configured)
priority 100
current priority 100
track-priority 5
hello-interval 1 sec
backup hello-interval 60 sec
advertise backup disabled
dead-interval 0 ms
preempt-mode true
virtual ipv6 address 10:20:1::100

device# show ipv6 vrrp-extended vrid 1

Interface 1/1
----------------
auth-type md5-authentication
VRID 1 (index 1)
interface 1/1
state master
administrative-status enabled
mode non-owner(backup)
virtual mac dddd.eeee.ffff (configured)
priority 100
current priority 100
track-priority 5
hello-interval 1 sec
backup hello-interval 60 sec
advertise backup disabled
dead-interval 0 ms
preempt-mode true
virtual ipv6 address 10:20:1::100
```

The following example displays group member information for the VRRP-E scaling feature for VRID 1. Only partial output is displayed.

```
device# show ipv6 vrrp-extended ve 100 vrid 1

VRID 2 (index 2)
 interface v100
 state backup
.
.
.
 group-member count 3
 group-members
   ve 100 vrid 2
   ve 100 vrid 3
   ve 100 vrid 4
```

The following example displays group master information for the VRRP-E scaling feature for interface ve 100 and VRID 2. Only partial output is displayed.

```
device# show ipv6 vrrp-extended ve 100 vrid 2

VRID 2 (index 2)
 interface v100
 state backup
.
.
.
 group-master ve 100 vrid 1
```

History

Release version	Command history
05.8.00	This command was modified to add new output for the VRRP-E scaling and VRRP-E multiple IP addresses features.

show isis

Displays general IS-IS information.

Syntax

show isis

Modes

User EXEC mode

Command Output

The **show isis** command displays the following information:

Output field	Description
IS-IS Routing Protocol Operation State	The operating state of IS-IS. Possible states include the following: • Enabled - IS-IS is enabled. • Disabled - IS-IS is disabled.
IS-Type	The intermediate system type. Possible types include the following: • Level 1 only - The device routes traffic only within the area in which it resides. • Level 2 only - The device routes traffic between areas of a routing domain. • Level 1-2 - The device routes traffic within the area in which it resides and between areas of a routing domain.
System ID	The unique IS-IS router ID. Typically, the device's base MAC address is used as the system ID.
Manual area address(es)	Area address(es) of the device.
Level-1-2 Database State	The state of the Level 1-2 Database: • On • Off
Administrative Distance	The current setting of the IS-IS administrative distance.
Maximum Paths	The number of paths IS-IS can calculate and install in the forwarding table
Default redistribution metric	The value of the default redistribution metric, which is the IS-IS cost of redistributing the route into IS-IS.
Number of Routes redistributed into IS-IS	The number of routes distributed into IS-IS.
Level-1 Auth-mode	One of the following authentication modes set for Level-1 on the router: • None • md5 • cleartext
Level-2 Auth-mode	One of the following authentication modes set for Level-2 on the router: • None • md5

Output field	Description
	• cleartext
Metric Style Supported for Level-1	The following values are supported: • Wide - Wide Metric Style • Narrow - Narrow Metric Style
Metric Style Supported for Level-2	The following values are supported: • Wide - Wide Metric Style • Narrow - Narrow Metric Style
IS-IS Partial SPF Optimizations	This parameter can contain one of the following values: • Enabled • Disabled
Timers: L1 or L2 SPF:	These values are displayed individually for IS-IS levels 1 and 2.
max-wait	The maximum time gap that occurs between running of SPF calculations. It is the value configured as the spf-max-wait variable in the**spf-interval** command.
Init-wait	The initial time gap between an SPF event and the first running of SPF. This value reflects the spf-initial-time variable that is configured using the **spf-interval** command.
Second-wait	The interval between the first running of SPF and the first recalculation of the SPF tree. If this optional value is configured, it is doubled with each recalculation of the SPF tree until the value is equal to the max-wait value This value reflects the spf-second-wait variable that is configured using the **spf-interval** command.
SPF run status.	This field is not specifically labeled but is displayed directly under the SPF timers. It can any of the three values shown below: • SPF is running • SPF will run in *sec* where the *sec* variable is a value in seconds until the next time that SPF will be run. • SPF is not scheduled
Timers: PSPF:	
max-wait	The maximum time gap that occurs between running of PSPF calculations. It is the value configured as the max-wait value in the**partial-spf-interval** command.
Init-wait	The initial time gap between the wait time after an LSP change until the first PSPF calculation. This value reflects the initial-wait variable that is configured using the **partial-spf-interval** command.
Second-wait	The wait time between the first and second PSPF calculations. If this optional value is configured, it is doubled with each PSPF recalculation until the value is equal to the max-wait value This value reflects the second-wait variable that is configured using the **partial-spf-interval** command.
PSPF run status.	This field is not specifically labeled but is displayed directly under the PSPF timers. It can any of the three values shown below: • PSPF is running • PSPF will run in *sec* where the *sec* variable is a value in seconds until the next time that PSPF will be run. • PSPF is not scheduled
Timers: LSP:	

Output field	Description
max-lifetime	The maximum number of seconds an unrefreshed LSP can remain in the device's LSP database. The default value is 1000 sec.
refresh-interval	The maximum number of seconds that a device waits between sending updated LSPs to its IS-IS neighbors. The default value is 1 sec.
gen-interval	The minimum number of seconds that a device waits between sending updated LSPs to its IS-IS neighbors. The default value is 10 sec.
retransmit-interval	The amount of time the device waits before it retransmits LSPs. The default value is 5 sec.
lsp-interval	The rate of transmission (in milliseconds) of the LSPs. The default rate is 33 ms.
Timers: SNP:	
csnp-interval	How often the designated IS sends a CSNP to the broadcast interface. The default value is 10 sec.
psnp-interval	How often the IS sends a PSNP. The default value is 2 sec.
Global Hello Padding	This value can be: • Enabled • Disabled
Global Hello Padding For Point to Point Circuits	This value can be: • Enabled • Disabled
Ptpt Three Way HandShake Mechanism	This value can be: • Enabled • Disabled
IS-IS Traffic Engineering Support	This value can be: • Enabled • Disabled
BFD	This value can be: • Enabled • Disabled
Interfaces with IPv4 IS-IS configured	Interfaces on which IPv4 IS-IS is configured.

Examples

This example displays sample output from the **show isis** command.

```
device# show isis

 IS-IS Routing Protocol Operation State: Enabled
IS-Type: Level-1-2
System ID: 0000.0011.1111
Manual area address(es):
47
Level-1-2 Database State: On
Administrative Distance: 115
Maximum Paths: 4
Default redistribution metric: 0
Protocol Routes redistributed into IS-IS:
Static
Number of Routes redistributed into IS-IS: 11
Level-1 Auth-mode: None
Level-2 Auth-mode: None
Metric Style Supported for Level-1: Wide
Metric Style Supported for Level-2: Wide
IS-IS Partial SPF Optimizations: Enabled
Timers:
L1 SPF: Max-wait 120s Init-wait 100ms Second-wait 120000ms
L2 SPF: Max-wait 100s Init-wait 100ms Second-wait 100000ms
L1 SPF is not scheduled
L2 SPF is not scheduled
PSPF: Max-wait 120000ms Init-wait 120000ms Second-wait 120000ms
PSPF is not scheduled
 LSP: max-lifetime 1200s, refresh-interval 900s, gen-interval 10s
retransmit-interval 5s, lsp-interval 33ms
SNP: csnp-interval 10s, psnp-interval 2s
Global Hello Padding : Enabled
Global Hello Padding For Point to Point Circuits: Enabled
Ptpt Three Way HandShake Mechanism: Enabled
IS-IS Traffic Engineering Support: Disabled
BFD: Disabled
Interfaces with IPv4 IS-IS configured:
eth 1/1
```

show isis config

Displays the global IS-IS configuration commands that are in effect on the device.

Syntax

show isis config

Modes

User EXEC mode

Usage Guidelines

The running-config does not list the default values. Only commands that change a setting or add configuration information are displayed.

Examples

This example displays sample output from the **show isis config** command.

```
device# show isis config

router isis
 auth-mode cleartext level-1
 auth-mode md5 level-2
 auth-key "********" level-1
 csnp-interval 22
 fast-flood 4
 log adjacency
 log invalid-lsp-packets
 disable-inc-stct-spf-opt
 address-family ipv4 unicast
 exit-address-family

 address-family ipv6 unicast
  summary-prefix 2001:db8::/32
 exit-address-family
```

show isis counts

Displays IS-IS error statistics.

Syntax

show isis counts

Modes

User EXEC mode

Command Output

The **show isis counts** command displays the following information:

Output field	Description
Area Mismatch	The number of times the device interface was unable to create a Level-1 adjacency with a neighbor because the device interface and the neighbor did not have any areas in common.
Max Area Mismatch	The number of times the device received a PDU whose value for maximum number of area addresses did not match the device's value for maximum number of area addresses.
System ID Length Mismatch	The number of times the device received a PDU whose ID field was a different length than the ID field length configured on the device.
LSP Sequence Number Skipped	The number of times the device received an LSP with a sequence number that was more than 1 higher than the sequence number of the previous LSP received from the same neighbor.
LSP Max Sequence Number Exceeded	The number of times the device attempted to set an LSP sequence number to a value higher than the highest number in the CSNP sent by the Designated IS.
Level-1 Database Overload	The number of times the Level-1 state on the device changed from Waiting to On or from On to Waiting. • Waiting to On - This change can occur when the device recovers from a previous Level-1 LSP database overload and is again ready to receive new LSPs. • On to Waiting - This change can occur when the device's Level-1 LSP database is full and the device receives an additional LSP, for which there is no room.
Level-2 Database Overload	The number of times the Level-2 state on the device changed from Waiting to On or from On to Waiting. • The change from Waiting to On can occur when the device recovers from a previous Level-2 LSP database overload and is again ready to receive new LSPs. • The change from On to Waiting can occur when the device's Level-2 LSP database is full and the device receives an additional LSP, for which there is no room.
Our LSP Purged	The number of times the device received an LSP that was originated by the device itself and had age zero (aged out).
PDU Drop Count	

Output field	Description
CSNP Auth Failures	The number of CSNP Authentication failures recorded for Level-1 and Level-2. This counter will only be displayed if it has a value greater than zero.
PSNP Auth Failures	The number of PSNP Authentication failures recorded for Level-1 and Level-2. This counter appears only if it has a value greater than 0.
HELLO Auth Failures	The number of HELLO Authentication failures recorded for Level-1 and Level-2. This counter will only be displayed if it has a value greater than zero.
Adjacency not found	The number of PDUs dropped at both Level-1 and Level-2 because there is no valid adjacency on the interface where they were received. This counter will only be displayed if it has a value greater than zero.
Adjacency Level Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the adjacency from which the PDU is received has a different level than the PDU level. This counter will only be displayed if it has a value greater than zero.
IS Level Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the IS-IS router level mismatches with the PDU level received. This counter will only be displayed if it has a value greater than zero.
Length Too Short	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU length is less than the standard PDU header length. This counter will only be displayed if it has a value greater than zero.
Length Too Long	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU length is greater than the MTU of the link. This counter will only be displayed if it has a value greater than zero.
Max Area Check Failure	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a maximum area count different than what is configured on this IS-IS router. This counter will only be displayed if it has a value greater than zero.
Zero Checksum	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a zero checksum. This counter will only be displayed if it has a value greater than zero.
Checksum Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a checksum different than the computed checksum on the received PDU. This counter will only be displayed if it has a value greater than zero.
Invalid Length	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a different length than what is advertised in the PDU header. This counter will only be displayed if it has a value greater than zero.

Examples

This example displays sample output from the **show isis counts** command.

```
device# show isis counts

Area Mismatch: 0
Max Area Mismatch: 0
System ID Length Mismatch: 0
LSP Sequence Number Skipped: 0
LSP Max Sequence Number Exceeded: 0
Level-1 Database Overload: 0
Level-2 Database Overload: 0
Our LSP Purged: 0
PDU Drop Count
CSNP Auth Failures : [L1: 100] [L2: 0]
PSNP Auth Failures : [L1: 100] [L2: 0]
HELLO Auth Failures : [L1: 100] [L2: 0]
Adjacency not found : [L1: 100] [L2: 200]
Adjacency Level Mismatch : [L1: 100] [L2: 200]
IS Level Mismatch : [L1: 100] [L2: 200]
Length Too Short : [L1: 100] [L2: 200]
Length Too Large : [L1: 100] [L2: 200]
Max Area Check Failure : [L1: 100] [L2: 200]
Zero Checksum : [L1: 100] [L2: 200]
Checksum Mismatch : [L1: 100] [L2: 200]
Invalid Length : [L1: 100] [L2: 200]
```

show isis database

Displays information about the entries in the LSP database.

Syntax

show isis database lsp-id [**detail**] [**level1**] [**level2**]

show isis database detail [**level1** | **level2**]

show isis database level1 [**detail**]

show isis database level2 [**detail**]

show isis database summary

Parameters

lsp-id

Specifies a link-state packet (LSP) in HHHH.HHHH.HHHH.HH-HH format, for example, 3333.3333.3333.00-00, or by entering a name, for example, XMR.00-00.

detail

Specifies detailed information.

level1

Specifies Level 1 packets only.

level2

Specifies Level 2 packets only.

summary

Specifies summarized information.

Modes

User EXEC mode

Command Output

The **show isis database** command displays the following information:

Output field	Description
LSPID	The LSP ID, which consists of the source ID (6 bytes), the pseudonode (1 byte), and LSPID (1 byte). NOTE If the address has an asterisk (*) at the end, this indicates that the LSP is locally originated.
LSP Seq Num	The sequence number of the LSP.
LSP Checksum	The checksum calculated by the device that sent the LSP and used by the device to verify that the LSP was not corrupted during transmission over the network.

Output field	Description
LSP Holdtime	The maximum number of seconds during which the LSP will remain valid. NOTE The IS that originates the LSP sets the timer for the LSP. As a result, LSPs do not all have the same amount of time remaining when they enter the device's LSP database.
ATT	A 4-bit value extracted from bits 4 - 7 in the Attach field of the LSP.
P	The value in the Partition option field of the LSP. The field can have one of the following values: • 0 - The IS that sent the LSP does not support partition repair. • 1 - The IS that sent the LSP supports partition repair.
OL	The value in the LSP database overload field of the LSP. The field can have one of the following values: • 0 - The overload bit is off. • 1 - The overload bit is on, indicating that the IS that sent the LSP is overloaded and should not be used as a IS-IS transit router for that level.
NLPID	The Network Layer Protocol Identifier (NLPID), which specifies the protocol the IS that sent the LSP is using. Usually, this value is "CC(IP)".
IP address	The IP address of the interface that sent the LSP. The device can use this address as the next hop in routes to the addresses listed in the rows below.
Destination addresses	The rows of information below the IP address row are the destinations advertised by the LSP. The device can reach these destinations by using the IP address listed above as the next hop. Each destination entry contains the following information: • Metric - The value of the default metric, which is the IS-IS cost of using the IP address above as the next hop to reach this destination. • Device type - The device type at the destination. The type can be one of the following: – End System - The device is an ES. – IP-Internal - The device is an ES within the current area. The IP address and subnet mask are listed. – IS - The device is another IS. The NET (NSAP address) is listed. – IP-Extended - Same as IP-Internal, except the device uses the extended TLV fields described in draft-ietf-isis-traffic-02.txt to carry the information. – IS-Extended - Same as IS, except the device uses the extended TLV fields described in draft-ietf-isis-traffic-02.txt to carry the information.
Flooding to *num* interface:	Identifies the number of interfaces on which the specific LSP entry will be flooded and identifies the interfaces.
Acking to *num* interface:	Identifies the number of interfaces on which the specific LSP entry will be acknowledged and identifies the interfaces.

Examples

The following is sample output for the **show isis database** command when no argument or keyword is used.

```
device> show isis database

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
XMR-1.00-00           0x0000000c   0xd048        963               1/0/0
XMR-1.01-00           0x00000004   0x09b0        957               0/0/0
XMR-1.02-00           0x00000001   0xc57b        961               0/0/0
XMR.00-00*            0x0000000b   0x23fb        1030              1/0/0
IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
XMR-1.00-00           0x0000000d   0x7d97        964               1/0/0
XMR-1.01-00           0x00000004   0x09b0        958               0/0/0
XMR-1.02-00           0x00000001   0x200f        962               0/0/0
XMR.00-00*            0x0000000b   0x5647        1030              1/0/0
0000.0100.0003.00-00  0x0000001f   0x761a        932               0/0/0
0000.0100.0003.00-01  0x0000001d   0x9c9d        606               0/0/0
```

The following is sample output for the **show isis database** command when the **detail** keyword is used.

```
device> show isis database detail

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
XMR.00-00*            0x0000000b   0x23fb        971               1/0/0
   Area Address:  49
   NLPID:  CC(IP)
   Hostname:  XMR14
   IP Address: 10.1.1.1
   IPv6 Address: 2001:db8::14
   Metric:  10    IP-Internal 10.1.1.0/24          Up-bit: 0
   Metric:  10    IS XMR.01
IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
XMR.00-00*            0x0000000d   0x7d97        903               1/0/0
   Area Address:  49
   NLPID:  IPv6IP
   Hostname:  XMR14
   IP address: 10.1.1.1
   IPv6 address: 2001:db8::14
   Flooding to 1 interface: eth 1/7
   Metric:  10    IP-Internal 10.1.1.0/24          Up-bit: 0
   Metric:  10    IP-Internal 10.85.1.0/24       Up-bit: 0
   Metric:  10    IS XMR.01
   Metric:  10    IS XMR.02
```

show isis hostname

Displays the router-name-to-system-ID mapping table entries for an IS-IS device.

Syntax

show isis hostname

Modes

User EXEC mode

Examples

This example displays sample output from the **show isis hostname** command.

```
device# show isis hostname

Total number of entries in IS-IS Hostname Table: 1
   System ID        Hostname            * = local IS
 * 0000.00cc.dddd   XMR
```

show isis interface

Displays information about IS-IS interfaces for a device.

Syntax

show isis interface

show isis interface brief

show isis interface ethernet *slot/port*

show isis interface loopback *number*

show isis interface tunnel *number*

show isis interface ve *vlan_id*

Parameters

brief
Specifies a brief summary of IP interface IS-IS interface information.

ethernet *slot* **/** *port*
Specifies an Ethernet slot and port.

loopback *number*
Specifies a loopback interface.

tunnel *number*
Specifies a tunnel interface.

ve *vlan_id*
Specifies a virtual Ethernet (VE) interface.

Modes

User EXEC mode

Command Output

The **show isis interface** command displays the following information:

Output field	Description
Total number of IS-IS interfaces	The number of interfaces on which IS-IS is enabled.
Interface	The port or virtual interface number to which the information listed below applies.
Circuit State	The state of the circuit, which can be one of the following: • DOWN • UP

Output field	Description
Circuit Mode	The IS-IS type in use on the circuit. The mode can be one of the following: • LEVEL-1 • LEVEL-2 • LEVEL-1-2
Circuit Type	The type of IS-IS circuit running on the interface. The circuit type can be one of the following: • BCAST (broadcast). • PTP (Point-to-Point)
Passive State	The passive state determines whether the interface is allowed to form an IS-IS adjacency with the IS at the other end of the circuit. The state can be one of the following: • FALSE - The passive option is disabled. The interface can form an adjacency with the IS at the other end of the link. • TRUE - The passive option is enabled. The interface cannot form an adjacency, but can still advertise itself into the area.
Circuit Number	The ID that the instance of IS-IS running on the interface applied to the circuit between this interface and the interface at the other end of the link.
MTU	The maximum length supported for IS-IS PDUs sent on this interface.
Level-1 Auth-mode	One of the following authentication modes set for Level-1 on the router: • None • md5 • cleartext
Level-2 Auth-mode	One of the following authentication modes set for Level-2 on the router: • None • md5 • cleartext This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.
Level-1 Metric	The default-metric value that the device inserts in IS-IS Level-1 PDUs for this interface.
Level-1 Priority	The priority of this IS to be elected as the Designated IS for Level-1 in this broadcast network.
Level-1 Hello Interval	The number of seconds the software waits between sending Level-1 hello PDUs to the IS at the other end of the circuit.
Level-1 Hello Multiplier	The number by which the software multiplies the hello interval to calculate the hold time set in Level-1 Hello PDUs sent on the circuit.
Level-1 Designated IS	The NET of the Level-1 Designated IS.
Level-1 DIS Changes	The number of times the NET of the Level-1 Designated IS has changed.
Level-2 Metric	The default-metric value that the device inserts in IS-IS Level-2 PDUs for this interface.

Output field	Description
Level-2 Priority	The priority of this IS to be elected as the Designated IS for Level-2 in this broadcast network.
Level-2 Hello Interval	The number of seconds the software waits between sending Level-2 Hello messages to the IS at the other end of the circuit.
Level-2 Hello Multiplier	The number by which the software multiplies the hello interval to calculate the hold time set for Level-2 Hello PDUs sent on this circuit. This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.
Level-2 Designated IS	The NET of the Level-2 Designated IS.
Level-2 DIS Changes	The number of times the NET of the Level-2 Designated IS has changed.
Next IS-IS LAN Level-1 Hello	Number of seconds before next Level-1 Hello PDU will be transmitted by the device.
Next IS-IS LAN Level-2 Hello	Number of seconds before next Level-2 Hello PDU will be transmitted by the device.
Number of active Level-1 adjacencies	The number of ISs with which this interface has an active Level-1 adjacency.
Number of active Level-2 adjacencies	The number of ISs with which this interface has an active Level-2 adjacency.
Circuit State Changes	The number of times the state of the circuit has changed.
Circuit State Adjacencies Changes	The number of times an adjacency has started or ended on this circuit.
Rejected Adjacencies	The number of adjacency attempts by other ISs rejected by the device.
Circuit Authentication L1 failures	The number of times the device rejected a circuit because the authentication did not match the authentication configured for Level 1 on the device.
Circuit Authentication L2 failures	The number of times the device rejected a circuit because the authentication did not match the authentication configured for Level 2 on the device. This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.
Bad LSP	The number of times the interface received a bad LSP from an IS at the other end of the circuit. The following conditions can cause an LSP to be bad: • Invalid checksum • Invalid length • Invalid lifetime value
Control Messages Sent	The number of IS-IS control PDUs sent on this interface.
Control Messages Received	The number of IS-IS control PDUs received on this interface.
Hello Padding:	The Hello Padding configuration, which can be: • Enabled

Output field	Description
	• Disabled
IP Enabled	If set to TRUE, the IP protocol is enabled for this circuit.
IP Address and Subnet Mask	The IP address and subnet mask for this interface.
IPv6 Enabled	If set to TRUE, the IPv6 protocol is enabled for this circuit.
IPv6 Address and Subnet Mask	The IPv6 address and subnet mask for this interface.
Ipv6 Link-Local Addresses	The IPv6 link local address for this interface.
MPLS TE Enabled:	If set to TRUE, MPLS Traffic Engineering protocol is enabled for this circuit.
BFD Enabled:	If set to TRUE, BiDirectional Forwarding Detection is enabled for this circuit.

Examples

The following example displays information about IS-IS interfaces for a device.

```
device# show isis interface

show isis interface                                  Total number of IS-IS Interfaces:
1
                   Interface: eth 1/1
Circuit State: UP Circuit Mode: LEVEL-1-2
Circuit Type: BCAST Passive State: FALSE
Circuit Number: 0x01, MTU: 1500
Level-1 Auth-mode: None
Level-2 Auth-mode: None
Level-1 Metric: 10, Level-1 Priority: 64
Level-1 Hello Interval: 5 Level-1 Hello Multiplier: 3
Level-1 Designated IS: mu2-01 Level-1 DIS Changes: 3
Level-2 Metric: 10, Level-2 Priority: 64
Level-2 Hello Interval: 5 Level-2 Hello Multiplier: 3
Level-2 Designated IS: mu2-01 Level-2 DIS Changes: 3
Next IS-IS LAN Level-1 Hello in 1 seconds
Next IS-IS LAN Level-2 Hello in 4 seconds
Number of active Level-1 adjacencies: 0
Number of active Level-2 adjacencies: 0
Circuit State Changes: 1 Circuit Adjacencies State Changes: 0
Rejected Adjacencies: 0
Circuit Authentication L1 failures: 0
Circuit Authentication L2 failures: 0
Bad LSPs: 0
Control Messages Sent: 63 Control Messages Received: 27
Hello Padding: Enabled
IP Enabled: TRUE
IP Addresses:
10.1.1.2/24
IPv6 Enabled: TRUE
IPv6 Addresses:
1000::1/32
IPv6 Link-Local Addresses:
fe80::200:ff:fe02:c000
MPLS TE Enabled: FALSE
```

show isis ipv6 spf-log

Displays IS-IS IPv6 link-state packet (LSP) logging information.

Syntax

show isis ipv6 spf-log

show isis ipv6 spf-log detail

show isis ipv6 spf-log level-1 [**detail**]

show isis ipv6 spf-log level-2 [**detail**]

Parameters

detail

Specifies detailed information.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

User EXEC mode

Command Output

The **show isis ipv6 spf-log** command displays the following information:

Output field	Description
When	When (in hours: minutes : seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	The time required to complete this SPF run, Elapsed time is normal clock time (not CPU time). Other options for this field are: • Running - the SPF is still running and the duration will be updated after the SFP has run. • Pending - the event is pending and another SPF will be run once the currently executing SPF has completed.
Nodes	The number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	The number of events that triggered this SPF run. When a topology change has occurred, multiple link-state packets (LSPs) are received in a short time. Since a router waits about 5 seconds before running a full SPF run, it can include all new information. This count includes the number of events (such as receiving new LSPs) that occurred while the router was waiting the 5 second interval before running full SPF.

Output field	Description
Last Trigger LSP	When a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue about the source of routing instability in an area. If multiple LSPs in a single level are causing SPF runs, only the LSP ID of the last received LSP is recorded.
Triggers	The reason that a full SPF calculations was triggered.
Alternate Route Check	PSPF deleted an IPv4 or IPv6 route. Full SPF must run to find the alternate route.
Route Change in L1 SPF Run	The L1 SPF run added or deleted an IPv4 or IPv6 route. The L2 SPF must run to accommodate this change.
LSP Purged	An LSP was purged. A full SPF calculation must process this change.
LSP Added	A new LSP has appeared in the database. A full SPF calculation is needed to process this new LSP.
Summary Address Change	A summary address configuration change has occurred.
Adjacency State Change	An adjacency was added or deleted.
Admin Distance Change	The administrative distance configuration has changed.
LSP Header Change	The LSP header (attached or overload bits) is changed.
IS Neighbor TLV Change	An IS neighbor TLV was added or deleted in an LSP.
Area Address TLV Change	The area address TLV changed.
Interface IP Address Change	The IP address configuration changed.
IP Address TLV Change	An IP address TLV changed in the LSP.
IPv6 Address TLV Change	An IPv6 address TLV changed in the LSP.
IS-IS Level Change	The IS-IS level configuration changed.
Interface Metric Change	The IS-IS interface metric configuration changed.
LSP Changed - PSPF Disabled	The LSP changed and PSPF is disabled.
LSP Overload Bit Change	The overload bit in the LSP header changed.
Interface State Change	The interface state changed to up or down.
Redist Prefix-List Change	The redistribution list configuration changed.
Redist Policy Change	The redistribution policy configuration changed.
Maximum Path Change	The IS-IS maximum path configuration changed.
IP Load Sharing Change	The IP load sharing configuration changed.
User Cleared IS-IS Route	The user cleared a specific IS-IS route.
User Cleared IS-IS Routes	The user cleared all IS-IS routes.
Neighbor NLPID Change	NLPID set is changed in received hellos.
ISIS Enable	IS-IS was enabled.
ISTCT_SPF Computation	The user issued the **disable-incremental-stct-spf-opt** command.
User Cleared IS-IS All	The user issued the **clear isis all** command.
Interface Config Change	ISIS was enabled or disabled on a port.
User Trigger	The user issued the **clear isis spf-trigger** command.
Recompute InterLeve Routes	The neighbor IS-type is changed either from L1 to L12 or L12 to L1
Exited Overload State	IS-IS exited from an overload condition.

show isis neighbor

Displays IS-IS neighbor information.

Syntax

show isis neighbor [**detail**]

Parameters

detail

Specifies detailed information.

Modes

User EXEC mode

Command Output

The **show isis neighbors** command displays the following information:

Output field	Description
Total number of IS-IS Neighbors	The number of ISs with which the device has formed IS-IS adjacencies.
System ID	The System ID of the neighbor or the hostname of the neighbor.
Interface	The device port or virtual interface attached to the neighbor.
SNPA	The Subnetwork Point of Attachment (SNPA), which is the MAC address of the device port or virtual interface attached to the neighbor.
State	The state of the adjacency with the neighbor. The state can be one of the following: • DOWN - The adjacency is down. • INIT - The adjacency is being established and is not up yet. • UP - The adjacency is up.
Holdtime	The neighbor's advertised hold time.
Type	The IS-IS type of the adjacency. The type can be one of the following: • ISL1 - Level-1 IS • ISL2 - Level-2 IS • ES - ES NOTE The device forms a separate adjacency for each IS-IS type. Thus, if the device has both types of IS-IS adjacencies with the neighbor, the display contains a separate row of information for each adjacency.
Pri	The priority of this IS to be elected as the Designated IS in this broadcast network.

Output field	Description
StateChgeTime	The amount of time that has passed since the adjacency last changed state.
Protocol	The routing protocol supported by the neighbor. The protocol can be one of the following: • MT-ISIS - Multi-Topology is enabled on the neighbor. • ISIS - Multi-Topology is not enabled on the neighbor.

The **show isis neighbors detail** command displays the following information:

Output field	Description
Total number of IS-IS Neighbors	The number of ISs with which the device has formed IS-IS adjacencies.
System ID	The System ID of the neighbor or the hostname of the neighbor.
Interface	The device port or virtual interface attached to the neighbor.
SNPA	The Subnetwork Point of Attachment (SNPA), which is the MAC address of the device port or virtual interface attached to the neighbor.
State	The state of the adjacency with the neighbor. The state can be one of the following: • DOWN - The adjacency is down. • INIT - The adjacency is being established and is not up yet. • UP - The adjacency is up.
Holdtime	The neighbor's advertised hold time.
Type	The IS-IS type of the adjacency. The type can be one of the following: • ISL1 - Level-1 IS • ISL2 - Level-2 IS • ES - ES NOTE The device forms a separate adjacency for each IS-IS type. Thus, if the device has both types of IS-IS adjacencies with the neighbor, the display contains a separate row of information for each adjacency.
Pri	The priority of this IS to be elected as the Designated IS in this broadcast network.
StateChgeTime	The amount of time that has passed since the adjacency last changed state.
3-Way Handshake TLV received	The received 3-way handshake TLV for the interface.
Area Address (es)	The address of the area.
Protocols Supported	The topology supported by the neighbor.
IP Address	The IP address assigned to the neighbor interface.
Adj Usage L1	The adjacency level used by the neighbor.
circuit ID	The ID of the IS-IS circuit running on the neighbor interface.
Protocol	The routing protocol supported by the neighbor. The protocol can be one of the following: • MT-ISIS - Multi-Topology is enabled on the neighbor. • ISIS- Multi-Topology is not enabled on the neighbor.

Examples

The following example displays information about IS-IS neighbors.

```
device# show isis neighbor

Total number of IS-IS Neighbors: 2
System ID      Interface SNPA                                    State Holdtime Type Pri StateChgeTime
Protocol
00e0.52b5.7800 Ether2/4 00e0.52b5.7843 UP    10
ISL2     64  0  :0 :16:8     M-ISIS
00e0.52b5.7800 Ether2/4 00e0.52b5.7843 UP    10
ISL1     64  0  :0 :16:8                ISIS
```

The following example displays detailed information about IS-IS neighbors.

```
device# show isis neighbor detail

Total number of IS-IS Neighbors:
1
                       System ID Interface SNPA State Holdtime Type Pri StateChgeTime Protocol
Core2 ve 501 0900.2b00.0005 UP    30       PTPT 127 0  :0 :46:41  M-ISIS
3-Way HandShake TLV received: circuit-id 2
Area Address(es): 00.0000
Adj Usage L1
Protocols Supported: IP IPv6
IP Address: 191.28.1.2, circuit-id 2
```

show isis routes

Displays the routes in the IS-IS route table.

Syntax

show isis routes [*ip-address subnet-mask* | *ip-address/prefix*]

Parameters

ip-address subnet-mask
Specifies an IP address and network mask.

ip-address/prefix
Specifies an IP address and prefix.

Modes

User EXEC mode

Command Output

The **show isis routes** command displays the following information:

Output field	Description
Total number of IS-IS routes	The total number of routes in the device's IS-IS route table. The total includes Level-1 and Level-2 routes.
Destination	The IP destination of the route.
Mask	The subnet mask for the destination address.
Cost	The IS-IS default metric for the route, which is the cost of using this route to reach the next-hop router to this destination.
Type	The route type, which can be one of the following: • L1 - Level-1 route • L2 - Level-2 route
Tag	The tag value associated with the route.
Path	The path number in the table. The IS-IS route table can contain multiple equal-cost paths to the same destination, in which case the paths are numbered consecutively. When IP load sharing is enabled, the device can load balance traffic to the destination across the multiple paths.
Next Hop IP	The IP address of the next-hop interface to the destination.
Interface	The device interface (port or virtual interface) attached to the next hop.
Flags	Values used by technical support for troubleshooting.

Examples

The following is sample output for the **show isis routes** command when no argument or keyword is used.

```
device> show isis routes

Total number of IS-IS routes: 173
Destination      Mask             Cost  Type Tag      Flags
10.0.0.0          255.255.255.0    21    L2   00000000 00000242
   Path: 1       Next Hop IP: 10.1.1.1          Interface: 7/1
10.0.0.0          255.255.255.255  30    L2   00000000 00000242
   Path: 1       Next Hop IP: 10.1.1.1          Interface: 7/1
10.0.0.1          255.255.255.255  30    L2   00000000 00000242
   Path: 1       Next Hop IP: 10.1.1.1          Interface: 7/1
10.0.10.0         255.255.255.0    30    L2   00000000 00000242
   Path: 1       Next Hop IP: 10.1.1.1          Interface: 7/1
```

show isis shortcut

Displays information about all IS-IS shortcuts configured on the device.

Syntax

show isis shortcut

show isis shortcut detail

show isis shortcut lsp *name* **detail**

Parameters

detail

Specifies detailed information.

lsp *name*

Specifies a link-state packet (LSP).

Modes

User EXEC mode.

Usage Guidelines

Only LSPs that are UP (administratively and operationally enabled in the MPLS domain) are kept in the database and displayed in the show command outputs. LSPs that are down are not kept in the database and are not displayed in the command outputs.

This command also operates in all modes.

Command Output

The **show isis shortcut** command displays the following information:

Output field	Description
Configured	The number of IS-IS shortcuts configured.
Up	The number of IS-IS shortcuts that are UP.
Announced	The number of IS-IS shortcuts that are advertised.
Name	The name of the IS-IS shortcut. When the name is longer than 11 characters, it wraps to the next line.
To	The LSP endpoint address.
Metric (SPF or Announce)	The metric used in the SPF calculation or the metric used in the advertisement of the IS adjacency TLV. The SPF metric can be one of the following: • The metric configured at the MPLS LSP configuration level. • The native IGP metric plus or minus (+ or -) the relative metric configured with the **shortcuts isis** command.

Output field	Description
	• The native IGP metric • A dash (-) denotes that the tunnel is not used in SPF calculations. The Announce metric can be one of the following: • 10 (the default announce metric) • The metric configured with the **announce-metric** keyword • A dash (-) denotes that the tunnel is not used in the IS adjacency TLV advertisement.
Announce	Indicates whether or not IS-IS shortcuts are advertised: • Yes - IS-IS shortcuts are advertised • No - IS-IS shortcuts are not advertised.
Tunnel Intf	The tunnel index of the LSP. This is assigned by MPLS whenever an LSP is created.

Examples

The following example shows the output of the **show isis shortcut** command.

```
device# show isis shortcut
Configured: 3, Up: 2, Announced: 1
Name        To          Metric          Announce  Tunnel
                       (SPF/Announce)            Intf
lsp tomu2   10.4.1.1    10/-            No        tnl1
lsp tomu3   10.3.1.1    -/-             Yes       tnl2
lsp toolong 10.20.1.1   10/10           Yes       tnl3
toreachmu3
```

The following example shows the **show isis shortcut detail** command.

```
device# show isis shortcut lsp tomu2 detail
lsp tomu2
 To 10.1.1.1, Used by SPF (10), Not Announced
 LSP metric: 10, Relative metric: -, Announce metric: -
 ISIS System Id for 10.4.1.1. is mu2.00-00
 Not announced due to configuration
Last notification from MPLS received 0hhm35s ago.
```

show isis spf-log

Displays IS-IS link-state packet (LSP) logging information.

Syntax

show isis spf-log

show isis spf-log detail

show isis spf-log level-1 [**detail**]

show isis spf-log level-2 [**detail**]

Parameters

detail

Specifies detailed information.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

User EXEC mode

Command Output

The **show isis spf-log** command displays the following information:

Output field	Description
When	When (in hours: minutes : seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	The time required to complete this SPF run, Elapsed time is normal clock time (not CPU time). Other options for this field are: • Running - the SPF is still running and the duration will be updated after the SFP has run. • Pending - the event is pending and another SPF will be run once the currently executing SPF has completed.
Nodes	The number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	The number of events that triggered this SPF run. When a topology change has occurred, multiple link-state packets (LSPs) are received in a short time. Since a router waits about 5 seconds before running a full SPF run, it can include all new information. This count includes the number of events (such as receiving new LSPs) that occurred while the router was waiting the 5 second interval before running full SPF.

Output field	Description
Last Trigger LSP	When a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue about the source of routing instability in an area. If multiple LSPs in a single level are causing SPF runs, only the LSP ID of the last received LSP is recorded.
Triggers	The reason that a full SPF calculations was triggered.
Alternate Route Check	PSPF deleted an IPv4 or IPv6 route. Full SPF must run to find the alternate route.
Route Change in L1 SPF Run	The L1 SPF run added or deleted an IPv4 or IPv6 route. The L2 SPF must run to accommodate this change.
LSP Purged	An LSP was purged. A full SPF calculation must process this change.
LSP Added	A new LSP has appeared in the database. A full SPF calculation is needed to process this new LSP.
Summary Address Change	A summary address configuration change has occurred.
Adjacency State Change	An adjacency was added or deleted.
Admin Distance Change	The administrative distance configuration has changed.
LSP Header Change	The LSP header (attached or overload bits) is changed.
IS Neighbor TLV Change	An IS neighbor TLV was added or deleted in an LSP.
Area Address TLV Change	The area address TLV changed.
Interface IP Address Change	The IP address configuration changed.
IP Address TLV Change	An IP address TLV changed in the LSP.
IPv6 Address TLV Change	An IPv6 address TLV changed in the LSP.
IS-IS Level Change	The IS-IS level configuration changed.
Interface Metric Change	The IS-IS interface metric configuration changed.
LSP Changed - PSPF Disabled	The LSP changed and PSPF is disabled.
LSP Overload Bit Change	The overload bit in the LSP header changed.
Interface State Change	The interface state changed to up or down.
Redist Prefix-List Change	The redistribution list configuration changed.
Redist Policy Change	The redistribution policy configuration changed.
Maximum Path Change	The IS-IS maximum path configuration changed.
IP Load Sharing Change	The IP load sharing configuration changed.
User Cleared IS-IS Route	The user cleared a specific IS-IS route.
User Cleared IS-IS Routes	The user cleared all IS-IS routes.
Neighbor NLPID Change	NLPID set is changed in received hellos.
ISIS Enable	IS-IS was enabled.
ISTCT_SPF Computation	The user issued the **disable-incremental-stct-spf-opt** command.
User Cleared IS-IS All	The user issued the **clear isis all** command.
Interface Config Change	ISIS was enabled or disabled on a port.
User Trigger	The user issued the **clear isis spf-trigger** command.
Recompute InterLeve Routes	The neighbor IS-type is changed either from L1 to L12 or L12 to L1
Exited Overload State	IS-IS exited from an overload condition.

Examples

The following is sample output for the **show isis spf-log** command when the **detail** keyword is used.

```
device# show isis spf-log detail

ISIS Level-1 SPF Log
When      Duration  Nodes  Count  Last-Trigger-LSP         Trigger
0h1m57s   0         3      2      mu1.00-00                Adjacency Change
 Ipv4 Route updates: 4000 Ipv6 Route updates: 0
     First Trigger: 0h1m45s       Adj TLV Changed in LSP mu2.00-00
     Last Trigger : 0h1m45s       Adj TLV Changed in LSP mu1.00-00
0h2m3s    0         3      2      mu2.00-00                New LSP
 Ipv4 Route updates: 4000 Ipv6 Route updates: 0
     First Trigger: 1h42m45s      Adjacency mu2 is added
     Last Trigger : 1h42m45s      New LSP mu2.00-00 Appeared in database
0h2m9s    0         0      3      mu1.00-00                New LSP
 Ipv4 Route updates: 4000 Ipv6 Route updates: 0
     First Trigger: 1h42m45s      Interface ve 3 is Up
     Last Trigger : 1h42m45s      New LSP mu1.00-00 Appeared in database
1h5m12s    0ms      0     1     XMR16.00-00          ISTCT_SPF Computation
ISIS Level-2 SPF Log
When      Duration  Nodes  Count  Last-Trigger-LSP          Trigger
0h2m9s    0         0      3      mu1.00-00                 New LSP
 Ipv4 Route updates: 4000         Ipv6 Route updates: 0
     First Trigger: 1h42m45s      Interface ve 3 is Up
     Last Trigger : 1h42m45s      New LSP mu1.00-00 Appeared in database
0h2m21s   0         0      6      mu1.00-00                 New LSP
 Ipv4 Route updates: 4000         Ipv6 Route updates: 0
     First Trigger: 1h42m45s      Interface eth 1/1 is Up
     Last Trigger : 1h42m45s      New LSP mu1.00-00 Appeared in database
0h3m21s   0         0      3      mu1.00-00                 Adjacency Change
 Ipv4 Route updates: 4000 Ipv6 Route updates: 0
     First Trigger: 1h42m45s      New LSP mu1.00-00 Appeared in database
     Last Trigger : 1h42m45s      Adj TLV is Changed in LSP mu1.00-00
```

show isis traffic

Displays information about IS-IS packet counts.

Syntax

show isis traffic

Modes

User EXEC mode

Command Output

The **show isis traffic** command displays the following information:

Output field	Description
Level-1 Hellos	The number of Level-1 hello PDUs sent and received by the device.
Level-2 Hellos	The number of Level-2 hello PDUs sent and received by the device.
Level-1 LSP	The number of Level-1 link-state PDUs sent and received by the device.
Level-2 LSP	The number of Level-2 link-state PDUs sent and received by the device.
Level-1 CSNP	The number of Level-1 Complete Sequence Number PDUs (CSNPs) sent and received by the device.
Level-2 CSNP	The number of Level-2 CSNPs sent and received by the device.
Level-1 PSNP	The number of Level-1 Partial Sequence Number PDUs (PSNPs) sent and received by the device.
Level-2 PSNP	The number of Level-2 PSNPs sent and received by the device.

Examples

The following is sample output for the **show isis traffic** command.

```
device# show isis traffic

                          Message Received     Message Sent
 Level-1 Hellos           1029                 115
 Level-2 Hellos           1027                 112
 Level-1 LSP              6                    3
 Level-2 LSP              6                    3
 Level-1 CSNP             0                    0
 Level-2 CSNP             0                    0
 Level-1 PSNP             107                  0
 Level-2 PSNP             107                  0
```

show license

Displays general information about all software licenses for all units in a device.

Syntax

show license [*license index*] [**slot** *number*]

Parameters

license index

Specifies the software license file.

slot *slot number*

Specifies the slot number of the module. The *slot number* can be from 1 through 32.

Modes

Privileged EXEC level.

Usage Guidelines

The command can be used to display software licensing information for all available Brocade product families supporting software-based licensing, including node and non-node locked licensing.

Command Output

The **show license** command displays the following information:

Output field	Description
Index	The index number specifies the software license file for a specific stack. The index number is generated by the member unit. The license hash number that uniquely identifies the license.
Package name	The package name for the license.
Lid	The license ID. This number is embedded in the Brocade device.
Slot	Indicates that the license is active in the specified slot for the line card.
Lid	The license ID. The number is embedded in the Brocade device.
License Type	Indicates whether the license is normal (permanent) or trial (temporary).
Status	Indicates the status of the license: • Valid - A license is valid if the LID matches the license ID of the device for which the license was

Output field	Description
	purchased, and the package name is recognized by the system. • Invalid - The LID does not match the license ID of the device for which the license was purchased. • Active - The license is valid and in effect on the device. • Not used - The license is not in effect on the device. • Expired - For trial licenses only, this indicates that the trial license has expired.
License Period	If the license type is trial (temporary), this field displays the number of days the license is valid. If the license type is normal (permanent), this field displays Unlimited.
Trial license information	Indicates the trial license information details as displayed in the **show license** command output. • days used - The number of days the trial license has been effect. • hours used - The number of hours the trail license has been in effect. • days left - The number of days left before the trial license expires. • hours left - The number of hours left before the trial license expires.

Examples

The following example output displays information for a Brocade MLXe unit with three licenses installed; the 20x10GbE-X2-Scaling-UPG license, 20x10G-WITH-1G-MODE-ONLY license, and the 20x10G-1GAND- 10G-MODE license.

```
device#show license
Index    Package Name              Lid          Slot     License Type   Status       License Period

1       20x10GbE-X2-Scaling-UPG   dsuFKHJiFKz   S7       normal        active       unlimited
2       20x10G-WITH-1G-MODE-ONLY  dsuFKHJiFKz   S7       normal        active       unlimited
3       20x10G-1G-AND-10G-MODE    dsuFKHJiFKz   S7       normal        active       unlimited
4       20x10GbE-X2-Scaling-UPG   dsuFIKFlSSS  S19       normal        active       unlimited
5       20x10G-WITH-1G-MODE-ONLY  dsuFIKFlBBB  S20       normal        active       unlimited
```

History

Release version	Command history
07.1.00	This command was introduced.
05.0.00	This command was introduced.

show load-balance mask-options

Displays information about masking options for ECMP and LAG index hash calculations.

Syntax

show load-balance mask-options [**ethernet** | **gtp** | **ip** | **ipv6** | **mpls** | **pbb** | *slot number*]

Parameters

ethernet
Displays the Ethernet mask options.

gtp
Displays the GPRS Tunneling Protocol (GTP) mask options.

ip
Displays the IPv4 address mask options.

ipv6
Displays the IPv6 address mask options.

mpls
Displays the MPLS mask options.

pbb
Displays the Provider Backbone Bridges (PBB) mask options.

slot number
Displays information about the specified slot number.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays information about the Ethernet mask options.

```
device# show load-balance mask-options ethernet
Mask Ethernet options -
Mask Source MAC is enabled on -
No Slots
Mask Destination MAC is enabled on -
No Slots
Mask Vlan is enabled on -
No Slots
Mask Inner-Vlan is enabled on -
No Slots
Mask ISID is enabled on
```

The following example displays information about the PBB mask options.

```
device# show load-balance mask-options pbb
Mask PBB options -
Mask PBB Customer L2 Header is enabled on -
All Slots
Mask PBB Customer IPv4/IPv6 Header is enabled on -
Slot 1
Slot 2 - NPID 1
```

The following example displays information about the IPv4 address mask options.

```
device#show load-balance mask-options ip 2
Mask IPv4 options -

  Mask Source address is enabled on -

  No Network Processors

  Mask Destination address is enabled on -

  No Network Processors

  Mask Source address before symmetric lb is enabled on -

  No Network Processors

  Mask Destination address before symmetric lb is enabled on -

  No Network Processors

  Mask Source L4 port is enabled on -

  No Network Processors

  Mask Destination L4 port is enabled on -

  No Network Processors

  Mask Protocol ID is enabled on -

  No Network Processors
```

History

Release version	Command history
5.4.00	This command was introduced.
5.9.00	This command was modified to include additional information while displaying the command output.

show macsec ethernet

Displays status information for the designated MACsec interface.

Syntax

show macsec ethernet *slot*/*port*

Parameters

slot/*port*

Interface for which MACsec status information is to be displayed. The interface is designated slot on the device and interface on the slot.

Modes

User EXEC mode

Usage Guidelines

It is recommended that you use the **clear macsec ethernet** command to clear previous results.

Examples

The following code sample shows details for ethernet interface 1/1.

```
device(config)#show macsec ethernet 1/1

Transmit SC
-----------
 SC state                 : Transmitting

 SA[0] :
 SA state                 : Transmitting
 Next PN                  : 94a16300


Receive SC
----------
 SCstate                  : Receiving

SA[0] :
 SA State                 : Receiving
 Next PN                  : 96a32071
```

History

Release version	Command history
5.8.00	This command was introduced.

show macsec statistics ethernet

Displays status information and secure channel statistics for the designated MACsec interface.

Syntax

show macsec statistics ethernet *slot* **/** *port*

Parameters

slot **/** *port*

Interface for which MACsec status information is to be displayed. The interface is designated slot on the device and interface on the slot.

Modes

User EXEC mode

Usage Guidelines

It is recommended that you use the **clear macsec ethernet** command to clear previous results for the **show macsec ethernet** command before re-executing it.

Examples

The following code sample shows details for ethernet interface 1/1. The interface is verifying MACsec frames and is providing strict replay protection.

```
Brocade(config)#show macsec statistics ethernet 1/1
Interface statistics
--------------------
rx Untagged Pkts          : 3                   tx Untagged Pkts          : 0
rx Notagged Pkts          : 0                   tx Too long Pkts          : 0
rx Bad Tag  Pkts          : 0
rx Unknown SCI Pkts       : 0
rx No SCI Pkts            : 0
rx Overrun Pkts           : 0

Transmit Secure Channels
------------------------

SC Statistics
  Protected Pkts          : 0                   Protected Octets          : 0
  Encrypted Pkts          : 3                   Encrypted Octets          : 144

SA[0] Statistics - In use
  Protected Pkts          : 3
  Encrypted Pkts          : 3


SA[1] Statistics
  Protected Pkts          : 0
  Encrypted Pkts          : 0


SA[2] Statistics
  Protected Pkts          : 0
  Encrypted Pkts          : 0


SA[3] Statistics
  Protected Pkts          : 0
  Encrypted Pkts          : 0


Receive Secure Channels
-----------------------

SC Statistics
  OK Pkts                 : 0                   Not Valid Pkts            : 0
  Unchecked Pkts          : 0                   Not using SA Pkts         : 0
  Delayed Pkts            : 0                   Unused SA Pkts            : 0
  Late Pkts               : 0                   Validated Octets          : 0
  Invalid Pkts            : 0                   Decrypted Octets          : 0

SA[0] Statistics - In use
  OK Pkts                 : 0                   Invalid Pkts              : 0
  Not using SA Pkts       : 0                   Unused SA Pkts            : 0


SA[1] Statistics
  OK Pkts                 : 0                   Invalid Pkts              : 0
  Not using SA Pkts       : 0                   Unused SA Pkts            : 0


SA[2] Statistics
  OK Pkts                 : 0                   Invalid Pkts              : 0
  Not using SA Pkts       : 0                   Unused SA Pkts            : 0


SA[3] Statistics
  OK Pkts                 : 0                   Invalid Pkts              : 0
```

```
    Not using SA Pkts       : 0                 Unused SA Pkts          : 0
```

History

Release version	Command history
5.8.00	This command was introduced.

show memory histogram

Displays task memory usage information.

Syntax

show memory histogram [**pool** *pool-id* | **below** *threshold-value* | **trace** *taskname*]

Parameters

pool *pool-id*

Specifies the display of memory histogram information for a specific memory pool. The valid range is 0-3, where "0" = OS, "1" = Shared, "2" = Global and "3" = User Private.

below *threshold-value*

Specifies the display of memory histogram information when available memory falls below the specified percentage (5, 10 or 20 percent).

trace *taskname*

Specifies the display of high CPU condition task traces.

Modes

User EXEC mode

Examples

The following example displays memory histogram information.

```
device# show memory histogram
HISTOGRAM MEMORY SEQUENCE INFO
------------------------------
 DURATION   : 60 s
 SEQ IDX    : 1
 TIME       : 2012.07.10-11:14:08.539
 AVAIL MEM : below 5 %
-------------------------------------------------------
POOL      Total Memory      Used Memory Available Memory
              (bytes)          (bytes)          (bytes)
-------------------------------------------------------
Global      2855272448       2843262976         12009472
-------------------------------------------------------
Task Name            Alloc-Number    Alloc-Size(bytes)
-------------------------------------------------------
main                         1355             28486529
itc                             4                  645
tmr                            63                10173
ip_rx                         425               396453
scp                           748             17995881
lpagent                        63                31309
console                       101              3515673
vlan                           44              5814177
mac_mgr                        40              2305485
mrp                            26                 8541
vsrp                           28                 8557
erp                            28                 8557
mxrp                           26                 7527
snms                          192               188337
rtm                            98             33724605
rtm6                          109              1918717
ip_tx                         151              1274437
rip                            70               323733
ospf_msg_task                  17                 7453
telnet_0                       28                 7689
telnet_1                       29                 7817
-------------------------------------------------------
```

History

Release	Command History
5.5.00	This command was introduced.

show metro mp-vlp-queue

Displays priority information about management processor virtual line card (MP-VLP) queues on Brocade NetIron CER Series devices.

Syntax

show metro mp-vlp-queue

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view statistics about messages from the MP are that are queued in the VLP to dequeue.

NOTE
If the Dequeue Time is less than 1 millisecond, it is not recorded in the **show metro mp-vlp-queue** statistics. The corresponding timestamp is also not recorded. The initial timestamp is shown as "0000.00.00-00:00:00.000".

Command Output

The **show metro mp-vlp-queue** command displays the following information:

Output field	Description
MP => VLP Queue	The queue priority: high, medium, or low.
Queue Size	The maximum amount of packet counts that the queue can handle at a given time.
Total Pkt Count	The total count of messages queued in each queue.
Current Pkt Count	The count of messages queued at a specific moment in each queue.
Pkt High WM	The maximum messages reached in the queue at any point of time.
Pkt drop Count	The amount of messages that were dropped because the queue was full.
Dequeue High WM(msec)	The longest period of time, in milliseconds, that a message remained in that queue.
Timestamp Pkt High WM(High)	The timestamp for the time when the high water mark for the number of messages in the high priority queue is reached.
Timestamp Pkt High WM(Medium)	The timestamp for the time when the high water mark for the number of messages in the medium priority queue is reached.
Timestamp Pkt High WM(Low)	The timestamp for the time when the high water mark for the number of messages in the low priority queue is reached.
Timestamp Dequeue Time HWM(High)	The timestamp for the time when the most delay is observed in the high priority queue.
Timestamp Dequeue Time HWM(Medium)	The timestamp for the time when the most delay is observed in the medium priority queue.
Timestamp Dequeue Time HWM(Low)	The timestamp for the time when the most delay is observed in the low priority queue.

Examples

This example shows sample output from the **show metro mp-vlp-queue** command. Three MP-VLP queues are shown with priority High, Medium and Low. The messages from the MP are queued in these queues for the VLP to dequeue.

```
LP-1# show metro mp-vlp-queue

MP => VLP Queue       :         High       Medium          Low
Queue Size            :         2000         2000         2000
Total Pkt Count       :      2160279            0     61210672
Current Pkt Count     :            0            0            0
Pkt High WM           :           13            0         1992
Pkt drop count        :            0            0            0
Dequeue Time HWM(msec):        12000            0        12675

Timestamp Pkt High WM(High)       : [          13]: 2015.02.25-08:07:16.533
Timestamp Pkt High WM(Medium)     : [           0]: 0000.00.00-00:00:00.000
Timestamp Pkt High WM(Low)        : [        1992]: 2015.02.25-08:07:17.223

Timestamp Dequeue Time HWM(High)  : [       12000]: 2015.02.25-08:07:17.230
Timestamp Dequeue Time HWM(Medium): [           0]: 0000.00.00-00:00:00.000
Timestamp Dequeue Time HWM(Low)   : [       12675]: 2015.02.25-08:07:17.800
```

This example shows sample output from the **show metro mp-vlp-queue** command after statistics have been cleared using the **clear metro mp-vlp-queue** command.

```
LP-1# show metro mp-vlp-queue

MP => VLP Queue       :         High       Medium          Low
Queue Size            :         2000         2000         2000
Total Pkt Count       :            0            0            0
Current Pkt Count     :            0            0            0
Pkt High WM           :            0            0            0
Pkt drop count        :            0            0            0
Dequeue Time HWM(msec):            0            0            0

Timestamp Pkt High WM(High)       : [           0]: 0000.00.00-00:00:00.000
Timestamp Pkt High WM(Medium)     : [           0]: 0000.00.00-00:00:00.000
Timestamp Pkt High WM(Low)        : [           0]: 0000.00.00-00:00:00.000

Timestamp Dequeue Time HWM(High)  : [           0]: 0000.00.00-00:00:00.000
Timestamp Dequeue Time HWM(Medium): [           0]: 0000.00.00-00:00:00.000
Timestamp Dequeue Time HWM(Low)   : [           0]: 0000.00.00-00:00:00.000
```

History

Release version	Command history
5.8.00a	This command was introduced.

show metro-ring

Displays the metro ring details.

Syntax

show metro-ring *ring-id* [**diagnostics**]

Parameters

ring-id

Displays the details of the metro ring specified by the ring ID.

diagnostics

Displays the diagnostic results for the specified metro ring.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

VSRP VRID configuration mode

Command Output

The **show metro-ring** *ring-id* **diagnostics** command displays the following information:

Output field	Description
Ring id	The metro ring ID.
Diag state	The state of ring diagnostics.
RHP average time	The average round-trip time for an Ring Hello Packet (RHP) packet on the ring. The calculated time has a granularity of 1 microsecond.
Recommended hello time	The hello time recommended by the software based on the RHP average round-trip time.
Recommended Prefwing time	The preforwarding time recommended by the software based on the RHP average round-trip time.
Diag frame sent	The number of diagnostic RHPs sent for the test.
Diag frame lost	The number of diagnostic RHPs lost during the test.

The **show metro-ring** *ring-id* command displays the following information:

Output field	Description
Ring id	The metro ring ID.
State	The state of MRP. The state can be enabled or disabled.

Output field	Description
Ring role	Whether this node is the master for the ring. The role can be master or member.
Master vlan	The ID of the master VLAN in the topology group used by this ring. If a topology group is used by MRP, the master VLAN controls the MRP settings for all VLANs in the topology group. The topology group ID is 0 if the MRP VLAN is not the master VLAN in a topology group. Using a topology group for MRP configuration is optional.
Topo group	The topology group ID.
Hello time	The interval, in milliseconds, at which the forwarding port on the ring master node sends RHPs.
Prefwing time	The number of milliseconds an MRP interface that has entered the preforwarding state will wait before changing to the forwarding state.
Ring interfaces	The ring interfaces in the device. If the interfaces are part of a LAG, only the primary ports of the groups are listed.
Interface role	The interface role can be one of the following: • primary – Master node - The interface generates RHPs. – Member node - The interface forwards RHPs received on the other interface (the secondary interface). • secondary - The interface does not generate RHPs. – Master node - The interface listens for RHPs. – Member node - The interface receives RHPs.
Forwarding state	Whether MRP forwarding is enabled on the interface. The forwarding state can be one of the following: • blocking - The interface is blocking Layer 2 data traffic and RHPs. • disabled - The interface is down. • forwarding - The interface is forwarding Layer 2 data traffic and RHPs. • preforwarding - The interface is listening for RHPs but is blocking Layer 2 data traffic.
Active interface	The physical interfaces that are sending and receiving RHPs. If a port is disabled, its state is shown as "disabled". If an interface is part of a LAG, the member port which comes up first is listed.
Interface Type	Shows if the interface is a regular port or a tunnel port.
RHPs sent	The number of RHPs sent on the interface. NOTE This field applies only to the master node. On non-master nodes, this field contains 0. This is because the RHPs are forwarded in hardware on the non-master nodes.
RHPs rcvd	The number of RHPs received on the interface. NOTE On most Brocade devices, this field applies only to the master node. On non-master nodes, this field contains 0. This is because the RHPs are forwarded in hardware on the non-master nodes. However, on the FastIron devices, the RHP received counter on non-master MRP nodes increments. This is because, on FastIron devices, the CPU receives a copy of the RHPs forwarded in hardware.
TC RHPs rcvd	The number of Topology Change RHPs received on the interface. A Topology Change RHP indicates that the ring topology has changed.
State changes	The number of MRP interface state changes that have occurred. The state can be one of the states listed in the Forwarding state field.

Examples

The following example displays the MRP diagnostics result on the master node.

```
device# show metro-ring 1 diagnostics
Metro Ring 1 - custA
=============
diagnostics results

Ring       Diag       RHP average     Recommended     Recommended
id         state      time(microsec)  hello time(ms)  Prefwing time(ms)
1          disabled   < 0             100             300

Diag frame sent      Diag frame lost
0                    0
```

The following example displays the output of the **show metro-ring** command.

```
device# show metro-ring 1
Metro Ring 1
=============
Ring     State     Ring     Master    Topo       Hello      Prefwing
id                 role     vlan      group      time(ms)   time(ms)
2        enabled   member   2         not conf   100        300
Ring interfaces    Interface role     Forwarding state   Active interface  Interface Type
ethernet 1/1/1     primary            disabled           none              Regular
ethernet 1/1/2     secondary          forwarding         ethernet 2        Tunnel
RHPs sent          RHPs rcvd       TC RHPs rcvd       State changes
3                  0                                                0                 4
```

show mmrp

Displays Multiple MAC Registration Protocol (MMRP) information.

Syntax

show mmrp [**ethernet** *slot*/*port* [**vlan** *vlan-id*]]

Parameters

ethernet *slot port*

Displays information for a specific Ethernet port.

vlan *vlan-id*

Displays information for a specific virtual LAN (VLAN).

Modes

User EXEC mode

Usage Guidelines

MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

Use this command without any options to review MMRP information for all ports and VLANs. Use the optional **ethernet** and **vlan** keywords to display specific information about interfaces and VLANs that are registered as MMRP members.

Examples

The following example shows MMRP information for Ethernet interface 1/1.

```
device> show mmrp ethernet 1/1
----------------------------------------------------------------------
MMRP Status:           Enabled
Join-timer(in ms):     500
Leave-timer(in ms):    1600
Leaveall-timer(in ms): 10000
Include-vlan:          100,200,300-500,666
P2p:                   Yes
----------------------------------------------------------------------
Port   Vlan   Mac-count
------------------------
1/1    100    3
1/1    200    1
```

The following example shows MMRP information for VLAN 100.

```
device> show mmrp ethernet 1/1 vlan 100
----------------------------------------------------------------------
MMRP Status:           Enabled
Join-timer(in ms):     500
Leave-timer(in ms):    1600
Leaveall-timer(in ms): 10000
Include-vlan:          100,200,300-500,666
P2p:                   Yes
----------------------------------------------------------------------
Port   Vlan   Mac-count
------------------------
1/1    100    3
```

show mmrp attributes

Displays Multiple MAC Registration Protocol (MMRP) attributes.

Syntax

show mmrp attributes [**ethernet** *slot*/*port* [**vlan** *vlan-id*]]

Parameters

ethernet *slot port*

Displays information for a specific Ethernet port.

vlan *vlan-id*

Displays information for a specific virtual LAN (VLAN).

Modes

User EXEC mode

Usage Guidelines

MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

Use this command to review the addresses that are attached to various ports (and optionally, VLANs) and determine the registration state and applicant status. If no keyword options are used, information about all interfaces and VLANs that are registered as MMRP members is displayed.

Examples

The following example displays the MMRP registered member states.

```
device> show mmrp attributes

Port   Vlan   Mac-address      Registrar   Registrar   Applicant
                               State       Mgmt        State
-------------------------------------------------------------------
1/1    100    011e.8300.3001   IN          Fixed       Quiet Active
1/5    100    011e.8300.3001   LV          Normal      Quiet Active
1/5    100    011e.8300.3001   MT          Normal      Quiet Active
1/1    200    011e.8300.3002   IN          Fixed       Quiet Active
```

The following example displays the MMRP information for Ethernet interface 1/1.

```
device> show mmrp attributes ethernet 1/1

Port   Vlan   Mac-address      Registrar   Registrar   Applicant
                               State       Mgmt        State
-------------------------------------------------------------------
1/1    100    011e.8300.3001   IN          Fixed       Quiet Active
1/1    200    011e.8300.3002   IN          Fixed       Quiet Active
```

The following example displays the MMRP information for VLAN 100.

```
device> show mmrp attributes ethernet 1/1 vlan 100

Port   Vlan   Mac-address      Registrar   Registrar   Applicant
                               State       Mgmt        State
-----------------------------------------------------------------
1/1    100    011e.8300.3001   IN          Fixed       Quiet Active
```

show mmrp config

Displays the Multiple MAC Registration Protocol (MMRP) configuration.

Syntax

show mmrp config

Modes

User EXEC mode

Usage Guidelines

MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

Use this command to review the MMRP parameters configured on this device.

Examples

The following example displays the parameters configured for MMRP on this device.

```
device> show mmrp config

mmrp enable
 mmrp include-vlan 100,200,300
 mmrp timer join 400 leave 1400 leave-all 10000
!
interface ethernet 1/1
   mmrp enable
   mmrp point-to-point
   mmrp timer join 500 leave 2000 leave-all 15000
   mmrp include-vlan 600,500,300
   enable
!
interface ethernet 1/3
   mmrp enable
   mmrp timer join 600 leave 2200 leave-all 20000
   enable
!
interface ethernet 1/5
   mmrp enable
   mmrp point-to-point
   mmrp timer join 500 leave 2000 leave-all 15000
   enable
```

show mmrp statistics

Displays Multiple MAC Registration Protocol (MMRP) statistics.

Syntax

show mmrp statistics [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*

Displays information for a specific virtual LAN (VLAN).

Modes

User EXEC mode

Usage Guidelines

MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

Use this command to review the statistics for MMRP members. If the vlan keyword option is used, statistics for the specified VLAN are displayed.

Examples

The following example displays all MMRP statistics for this device.

```
device> show mmrp statistics

Vlan 100 - Ports 1/1 to 1/5
-------------------------------------
Message type   Received   Transmitted
-------------------------------------
In             0          0
Join In        0          0
Join Empty     0          0
Empty          0          156
Leave          0          0
Leave All      40         41
-------------------------------------
Total PDUs     2          826
-------------------------------------
Vlan 200 - Ports 2/1 to 2/5
-------------------------------------
Message type   Received   Transmitted
-------------------------------------
In             0          0
Join In        0          0
Join Empty     0          0
Empty          0          156
Leave          0          0
Leave All      40         41
-------------------------------------
Total PDUs     2          826
-------------------------------------
```

The following example displays MMRP statistics only for VLAN 100.

```
device> show mmrp statistics vlan 100

Vlan 100 - Ports 1/1 to 1/6
-----------------------------------
Message type   Received   Transmitted
-----------------------------------
In             0          0
Join In        0          0
Join Empty     0          0
Empty          0          156
Leave          0          0
Leave All      40         41
-----------------------------------
Total PDUs     2          826
-----------------------------------
```

show mpls autobw-threshold-table

Displays the global-threshold table.

Syntax

show mpls autobw-threshold-table

Modes

User EXEC mode

Usage Guidelines

This command displays the global-threshold table with the range of current-bandwidth and the corresponding absolute adjustment-threshold.

This command operates in all modes.

Command Output

The **show mpls autobw-threshold table** command displays the following information:

Output field	Description
Range (kbps)	Auto-bandwidth range in kilobytes per second.
Threshold (kbps)	Auto-bandwidth threshold in kilobytes per second.

Examples

The following example shows the **show mpls autobw-threshold-table** command.

```
device# show mpls autobw-threshold-table
Auto-bandwidth threshold table
 Range(kbps)           Threshold(kbps)
 0-10                        2000
 11-1000                  3000
 1001-10000            5000
 10001-max                10000
```

History

Release	Command history
5.6.00	The command was introduced.

show mpls bypass-lsp

Displays all dynamic bypass LSPs along with static bypass LSPs.

Syntax

show mpls bypass-lsp [**brief** | **wide** | **detail** | **name** *lsp_name* **extensive** [**descending**] | **invalid-tunnel-interface**

show mpls bypass-lsp { **up** | **down** } { **detail** | **extensive** [**descending**] | **wide** }

show mpls bypass-lsp { **dynamic** | **static** } { **brief** | **detail** | **extensive** [**descending**] | **interface** { **ethernet** *slot* / *port* { **brief** | **wide** } | **pos** *slot* / *port* { **brief** | **wide** } | **ve** *ve-id* { **brief** | **wide** } } }

Parameters

brief

Displays brief information.

detail

Displays detailed information.

wide

Displays long LSP names.

name

Displays LSP by name.

lsp_name

Selected LSP to display.

extensive

Displays detailed information with History.

descending

Displays detailed information with History in reverse chronological order.

invalid-tunnel-interface

Displays LSPs with an invalid tunnel-interface.

up

Displays operationally UP LSPs.

down

Displays operationally DOWN LSPs.

detail

Displays operationally UP/DOWN LSP detailed information.

extensive

Displays operationally UP/DOWN LSP detailed information with History.

descending

Displays operationally UP/DOWN LSPs History in reverse chronological order.

wide

Displays operationally UP/DOWN LSP long names.

dynamic
Displays dynamic bypass LSPs.

static
Displays static bypass LSPs.

brief
Displays dynamic/static LSP brief information.

detail
Displays dynamic/static LSP detailed information

extensive
Displays dynamic/static LSP detailed information with History.

descending
Displays detailed information with History in reverse chronological order.

interface
Displays dynamic/static LSP protected interface.

ethernet *slot* / *port*
Specifies an ethernet port.

pos *slot* / *port*
Specifies a POS port.

ve *ve-id*
Specifies a virtual interface (VE).

Modes

User EXEC mode

Examples

The following example displays the command with the brief option.

```
device# show mpls bypass-lsp dynamic brief
Note: LSPs marked with + are Dynamic Bypass LSPs
                          Admin Oper  Tunnel   Up/Dn Retry Active
Name        To            State State Intf     Times No.   Path
blsp01      22.22.22.22   UP    UP+   tnl1     1     0     bypas_path_1
_2
```

The following example displays that the non-brief versions include the tunnel-interface index.

```
device#show mpls bypass detail
LSP byp1, to 3.3.3.3, Tunnel interface index: 5002
  From: 120.120.120.2, admin: UP, status: DOWN (CSPF fails: Excluded MPLS interface is down)
  Times primary LSP goes up since enabled: 0
  Maximum retries: NONE, no. of retries: 0
  Pri. path: NONE, up: no, active: no
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  CSPF-computation-mode configured: use te-metric(global)
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: no
   Path calculated using interface constraint: no
   Path cspf-group computation-mode: disabled, cost: 0
  Tie breaking: random, hop limit: 0
  Exclude interface(s): e3/1
  Active Path attributes:
   Tunnel index: 65535
```

The following example displays information about the specified bypass-lsp using the **show mpls bypass-lsp name** *name* command.

```
device# show mpls bypass-lsp name t100
LSP t100, to 10.1.1.1
  From: 10.2.2.2, admin: UP, status: UP
  Times primary LSP goes up since enabled: 1
  Metric: 0, number of installed aliases: 0   Adaptive
  Maximum retries: NONE, no. of retries: 0
  Pri. path: NONE, up: no, active: no
  Setup priority: 7, hold priority: 0 ReoptimizeTimer: 300
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: no
   Path calculated using interface constraint: no
  Tie breaking: random, hop limit: 0
  Active Path attributes:
```

History

Release version	Command history
5.4.00	This command was modified to include filtering based of static bypass types, dynamic bypass types, and protected interface.
5.6.00	This command was modified to display the cspf-computation mode for the LSP at the local level. This is applicable to bypass LSPs, as well as dynamic bypass LSPs.
5.8.00	This command was modified to include the **descending** keyword.
5.9.00	This command was modified to include the tunnel-interface index in the display output for all non-brief versions.

show mpls config

Displays user-configured MPLS parameters.

Syntax

show mpls config autobw-template *autobw_template_name* | **autobw-threshold-table** | **brief** | **cspf-group** *cspf_group_name* | **dynamic-bypass** | **lsp** *lsp_name* | **path** *path_name* | **rsvp** | **static-lsp** *transit* | **vll** *vll_name* | **vll-local** *vll_local_name* | **vpls** *vpls_name*

show mpls config vpls [*vpls_id* | *vpls_name*]

show mpls config interface [**ethernet** *slot/port* | **pos** *slot/port* | **tunnel** *tunnel_id* | **ve** *num*]

show mpls config use-bypass-liberal

Parameters

autobw-template *autobw_template_name*
Displays the named automatic bandwidth template configuration information.

autobw-threshold-table
Displays autobw-threshold-table.

brief
Displays brief MPLS configuration information.

cspf-group *cspf_group_name*
Displays the named cspf-group configuration information.

dynamic-bypass *dynamic_bypass_name*
Displays the named dynamic bypass configuration information.

interface
Displays interface MPLS configuration information.

ethernet *slot/port*
Display the named ethernet port information.

pos *slot/port*
Displays the named POS port information.

tunnel *tunnel_id*
Displays the named tunnel interface information.

ve *num*
Displays the named virtual ethernet (VE) interface information.

lsp *lsp_name*
Displays the named LSP configuration information.

path *path_name*
Displays the named MPLS path configuration information.

rsvp
Displays all RSVP global configurations.

static-lsp *static_lsp_name*
Displays the named MPLS static LSPs configuration information.

use-bypass-liberal
Displays liberal mode as part of the command.

vll *vll_name*
Displays the named VLL configuration information.

vll-local *vll_local_name*
Displays the named VLL-local configuration information.

vpls *vpls_name*
Displays the named VPLS configuration information.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **show mpls config** with the optional **brief** keyword to display the prefix list configuration, instead of the ACL.

This command displays the MPLS configuration that exists for each of the keyword/variable options.

The **show mpls config use-bypass-liberal** command operates under the MPLS router mode (config-mpls-policy).

Examples

The following example shows the **show mpls config brief** command.

```
device show mpls config
device(config t)#
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)#
device(config-mpls-policy)# ingress-tunnel-accounting
device(config-mpls-policy)# auto-bandwidth sample-interval 300
device(config-mpls-policy)# ldp
device(config-mpls-ldp)# advertise-fec list-abc
```

The following example shows the output was modified to the overload bit configuration.

```
device# show mpls config
device(config t)#
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-1
device(config-mpls-policy)# handle-isis-neighbor-down
device(config-mpls-policy)# cspf-computation-mode ignore-overload-bit
```

The following example displays the configuration output for LSPs and bypass LSPs. They now show the tunnel interface index as part of the output.

```
lsp c2
 to 3.3.3.3
 tunnel-interface 5001
 enable

bypass-lsp byp1
 to 3.3.3.3
 exclude-interface  e3/1
 tunnel-interface 5002
 enable
```

History

Release	Command history
5.5.00	This command was modified to display the label withdrawal delay setting.
5.6.00	This command was modified to display the outbound FEC filter configuration parameter. This command was modified to include **use-bypass-liberal** under the cspf-computation-mode command output line.
5.7.00	This command was modified to display the prefix-list configuration instead of the ACL.
5.8.00	This command was modified to include the line "backup-bw-best-effort" in the **show mpls config rsvp** command output display.
5.9.00	This command was modified to include the next available RSVP LSP tunnel interface index.

show mpls forwarding

Displays the MPLS forwarding behavior when the router receives a labeled packet.

Syntax

show mpls forwarding *ip_prefix_addr* **longer**

show mpls forwarding in-label *in_label*

show mpls forwarding p2p *ip_addr*

show mpls forwarding p2mp [*dest_prefix* **detail** *in_label p2mp_id*]

Parameters

ip_prefix_addr

Displays P2P forwarding entries for the given destination.

longer

Displays P2P forwarding entries for the given destination with longer match.

in-label

Displays the P2P forwarding entry.

in_label

Specifies the selected in-label.

p2p

Displays all P2P forwarding entries for the specified destination or a specified in-label value.

ip_addr

Displays P2P forwarding entries for the given destination.

p2mp

Displays all P2MP forwarding entries.

dest_prefix

Specifies the selected destination prefix.

detail

Displays all P2MP forwarding entries in a detailed format.

in_label

Specifies the selected in-label to display.

p2mp_id

Specifies the selected P2MP to display.

Modes

User EXEC mode

Usage Guidelines

Command Output

The **show mpls forwarding** command displays the following information:

Output field	Description
Dest-prefix	The destination FEC of the LSP.
In-lbl	The incoming segment or upstream label for the LSP. A value of 0 indicates the absence of the segment.
Out-lbl	The outgoing segment or downstream label for the LSP.
Out-intf	The interface through which the label identified in the 'out-lbl' column has been distributed for the LSP. The 'out-intf' field displays whether an interface/port is an Ethernet port, POS port, or a VE interface. The VE interface ID specified by the *vid* variable. The out-intf display format for the interface/port is as follows: • [e | p] slot/port – 'e' represents an Ethernet port. – 'p' represents a POS port.
Sig	The signal protocol type associated with the label. Possible values are: • L - LDP • R - RSVP
Next-hop	The next hop of the LSP.
Type	The 'Type' field identifies a P2MP LSP.

Examples

The following example displays the output of the **show mpls forwarding** command.

```
device# show mpls forwarding
Total number of MPLS forwarding entries: 5
      Dest-prefix      In-lbl  Out-lbl  Out-intf   Sig  Next-hop    Type
1     80.80.80.80/32   1024    1500     e1/12      R    12.12.12.7
2     80.80.80.80/32   1025    1502     e1/11      R    11.11.11.7
3     80.80.80.80/32   1026    1503     e1/12      R    12.12.12.7
4     70.70.70.70/32   1027    3        e1/11      R    11.11.11.7
5     70.70.70.70/32   1028    3        e1/12      R    12.12.12.7
```

History

Release version	Command history
4.1.00	This command was introduced.
5.1.00	This command was modified to so the 'out-intf' field displays whether an interface/port is either Ethernet or POS.
5.5.00	This command CLI command syntax changed to **show mpls forwarding** and includes the options in the parameter section.

show mpls interface

Displays the details about a specific interface.

Syntax

show mpls interface [**brief** | **ethernet** *slot/port* | **pos** *slot/port* | **pos** *slot/port* | **tunnel** *tunnel_id* | **ve** *vid*]

Parameters

brief

Displays brief interface information.

ethernet *slot/port*

Specifies the Ethernet port information to display.

pos *slot/port*

Specifies the POS port information to display.

tunnel *tunnel_id*

Specifies the Tunnel interface information to display.

ve *vid*

Specifies the Virtual Ethernet (VE) interface information to display.

Modes

User EXEC mode.

Usage Guidelines

This command operates in all modes.

Command Output

The **show mpls interface ethernet** command displays the following information:

Output field	Description
Interface	The interface type refers to any one of the following: • Use the **ethernet** *slot/port* to limit the display to a single Ethernet port. • Use the **pos** *slot/port* to limit the display to a single POS port. • Use the **ve** *vid* to limit the display to a VE interface ID specified by the *vid* variable.
Maximum BW	The maximum outbound bandwidth that can be used on the interface. This TLV reflects the actual physical bandwidth of the interface.
Maximum reservable BW	The maximum reservable bandwidth on the interface. By default, the maximum reservable bandwidth is the same as the maximum bandwidth for the interface. The user can optionally change the reservable bandwidth on the interface by using the **reservable-bandwidth percentage** *num* command. The maximum reservable bandwidth displays as either an absolute value or a percentage value of the total interface bandwidth. In the show output displayed above, the maximum reservable bandwidth is configured as a percentage value. However, the

Output field	Description
	percentage value and the absolute value both display in the **show mpls interface ethernet** *slot/port* command output so that the user is aware that the bandwidth is configured as a percentage value, not an absolute value. NOTE When the maximum reservable bandwidth is configured as an absolute value, the percentage value is not displayed in the output of the **show mpls interface ethernet** *slot/port* command. Only the absolute value displays in the output.
Admin group	The administrative groups to which this interface belongs, set with the admin-group command.
Reservable BW [priority] kbps	The amount of bandwidth not yet reserved on the interface. Eight octets are displayed, indicating the amount of unreserved bandwidth (in kbps) that can be reserved with a hold priority of 0 through 7. The value in each of the octets is less than or equal to the maximum reservable bandwidth.
Last sent reservable BW [priority] kbps	The values in the Unreserved Bandwidth TLV sent in the most recent OSPF-TE LSA. When the device is not sending out OSPF-TE LSAs for the interface, the unreserved bandwidth value for each of the priorities is zero (0).
Configured Protecting bypass LSPs	The name and operational state of any bypass LSPs that are protecting this interface.

Examples

The following example shows the **show mpls interface ethernet** command:

```
device# show mpls interface ethernet 1/1
e1/1
Admin: Up  Oper: Up
  Maximum BW: 10000000 kbps, maximum reservable BW: 8000000 kbps (80%)
  Admin group: 0x00000000
  Reservable BW [priority] kbps:
   [0] 8000000    [1] 8000000    [2] 8000000    [3] 8000000
   [4] 8000000    [5] 8000000    [6] 8000000    [7] 8000000
  Last sent reservable BW [priority] kbps:
   [0] 8000000    [1] 8000000    [2] 8000000    [3] 8000000
   [4] 8000000    [5] 8000000    [6] 8000000    [7] 8000000
  Configured Protecting bypass lsps: 1
```

show mpls label-range

Displays the MPLS label ranges.

Syntax

show mpls label-range

Modes

This command operates under all modes.

Usage Guidelines

For an MPLS label, the label range must be between 16 and 499999.

Configuration of in-label values outside of the label range is not permitted.

When the label range is increased or reloaded, there is nothing to be handled. The user gets a wider label range to use.

When the label range is shortened or shifted, and when there are existing static LSPs that have in-labels that fall under the old range—but no longer under the new range—the following guidelines apply:

- They continue to stay UP as the label range change takes effect only after reload.
- When the user reloads with a configuration, that is, with some in-labels now outside of the label range, those LSPs do not come UP if they were or are enabled. However, they remain in the configuration.
- They are allowed to stay in the configuration only so that if the user re-configures the label range to include them and reloads, they can come UP. Also, removing from the configuration due to errors is incorrect behavior.
- The user can disable or enable the LSPs, but they do not come UP.
- The user cannot change the in-labels to another value outside the range, as per point 1 above. If the user changes any in-label successfully to a value inside the range, the user cannot change it back to the old outside-the-range value again. This to follows from point 1.
- When there are LSPs in the configuration that have an in-label value outside the static range, point 3 is the only way the user is able to end up in that state. User configuration of the in-label is not allowed to go outside the range.

Command Output

The **show mpls label-range** command displays the following information:

Output field	Description
MPLS label range	The header for the label ranges configured using commands **label-range** [**static** | **dynamic**] **min-value** *value* **max-value** *value*.
Static	Represents the static label range for transit labels.
Dynamic	Represents the dynamic label range for transit labels.
Modified label range	This header displays the values that have been configured, but not yet effective as label range changes require a reload. This section is visible only if a different set of values have been configured to take effect after reload.

Examples

Example of the **show mpls label-range** command display:

```
device# show mpls label-range
MPLS label range:
        Static             = 16 - 3000
        Dynamic            = 3001 - 499999
Modified label range:*
        Static             = 16 - 5000
        Dynamic            = 5001 - 499999
*These values will become effective after reload with saved config.
```

show mpls ldp

Displays the inbound FEC-filter configuration.

Syntax

show mpls ldp

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the inbound FEC-filter configuration.

```
device# show mpls ldp
Label Distribution Protocol version 1
 LSR ID:10.122.122.122,using Loopback 1 (deleting stops LDP)
 Hello interval: Link 5 sec, Targeted 15 sec
 Hello time value sent in Hellos: Link 15 sec, Targeted 45 sec
 Keepalive interval: 10 sec, Hold time multiple: 3 intervals
 Keepalive timeout: 30
 Inbound FEC filtering prefix-list list-abc
 Tunnel metric: 0
 FEC used for auto discovered peers: current 129, configured 129
 Label Withdrawal Delay: 30s
 Graceful restart: disabled
  Reconnect time: 0 seconds, Max peer reconnect time: 120 seconds
  Recovery time: 0 seconds, Max peer recovery time: 120 seconds
  Forwarding state holding timer: not running
 Label Withdrawal Delay: 30s
```

History

Release version	Command history
5.5.00	This command was modified to display the label withdrawal delay setting.

show mpls ldp database

Displays the contents of the LSRs LDP Label Information database.

Syntax

show mpls ldp database [*ip_addr*] [**filtered**]

Parameters

ip_addr

Displays the specified peer ID address.

filtered

Displays sessions with filtered mappings.

Modes

User EXEC mode

Usage Guidelines

This database contains all the labels it has learned from each of its LSR peers, as well as all of the labels it has sent to its LDP peers.

This command operates in all modes.

Command Output

The **show mpls ldp database** command displays the following information:

Output field	Description
Session	The LDP identifiers of this LSR and its peer.
Downstream label database	Information about labels received from the LDP peer.
Upstream label database	Information about labels distributed by this LSR to the LDP peer. The device sends the same label for a given prefix to all of its upstream peers.
Label	The label value received from or distributed to LDP peers. It also displays the label values for VC FECs received from LDP peers or advertised to upstream LDP peers.
Prefix	The destination route associated with the label. Since the Prefix is not applicable to the VC-FECs, this field indicates that the label is associated with the VC FEC.
State	Whether the label is actively being used for data forwarding. It can be one of the following: • 'Installed' indicates that the label is being used with an active LDP-created LSP to forward packets. • 'Retained' indicates that the label is not being used for packet forwarding. Since the LSRs use Liberal Label Retention, these unused labels are retained in the database and not discarded.

Examples

The following example displays the output of the **show mpls ldp database** command.

```
device# show mpls ldp database
Session 10.210.210.21:0 - 10.2.2.2:0
 Downstream label database:
  Label   Prefix                 State

 Upstream label database:
  Label   Prefix                 State
  1024    10.125.125.25/32(Stale)
  3       10.210.210.21/32(Stale)
  1025    10.220.220.22/32(Stale)

Session 10.210.210.21:0 - 10.220.220.22:0
 Downstream label database:
  Label   Prefix                 State
  3       10.220.220.22/32       Installed
  1024    10.125.125.25/32       Installed
  983097  VC-FEC                 Retained

Upstream label database:
  Label   Prefix
  3       10.210.210.21/32
  983040  VC-FEC
```

show mpls ldp fec

Displays MPLS forwarding equivalence class (FEC) information.

Syntax

show mpls ldp fec [**summary** | **vc** *vc_id*

show mpls ldp fec prefix [*ip_addr* | *ip_addr* **/** *subnet-mask-length* | **filtered** [**in** | **out**] | **prefix-filter** *prefix-list-name*]

Parameters

summary

Displays LDP FEC summary information.

vc *vc_id*

Displays a detailed view of the FEC VC specified by the *vc_id* variable.

prefix

Displays Layer 3 prefix FEC information.

ip_addr **/** *subnet-mask-length*

Specifies an IP address, with the option of adding subnet mask length.

filtered

Displays only filtered mapping configuration information.

in

Specifies inbound information.

out

Specifies outbound information.

prefix-filter prefix-list-name

Displays the FEC prefixes filtered by the specified prefix-list name.

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show mpls ldp fec** command options display the following information:

Output field	Description
Total number of prefix FECs	The total number of Layer 3 FECs.
Total number of prefix FECs installed	The total number of Layer 3 FECs installed.
Total number of prefix FECs filtered(in/out)	The total number of Layer 3 FECs filtered.

Output field	Description
Total number of prefix FECs with LWD timer running	The total number of Layer 3 FECs with LWD timer running.
Destination	The IP Prefix associated with the host address or the prefix FEC type.
State	State of the FEC which indicates the FEC advertised to any LDP session (state equal to 'current'. When it has no session, it is either called 'cur_no_sess' (currently no session) for local FECs or is marked "retained" for non-local FECs.
Out-intf	For an ingress FEC, this mentions the output interface to reach to the Next-hop. The 'Out-Intf' field displays the egress interface associated with the FEC entry. When applicable, the 'Out-Intf' field displays a VC interface specified by the *vc_id* variable.
Next-hop	For an ingress FEC, this mentions the next-hop IP address.
Ingress	Whether the FEC is an ingress FEC.
Egress	Whether the FEC is an egress FEC.
Filtered	The FEC is filtered Inbound (In) or Outbound (Out) or is not filtered (-).
LWD	Indicate if the Label withdrawal delay timer is active for the FEC.
LDP FEC summary	Summarized information for LDP FEC.
Total number of prefix FECs	The total number of prefix FECs in the LDP FEC database.
Total number of VC-FEC type 128	The total number of VC FECs for type 128. The FEC type for VC FEC can be 128 or 129.
Total number of VC-FEC type 129	The total number of VC FECs for type 129. The FEC type for VC FEC can be 128 or 129.
Total number of route update processing errors	The total number of route update processing errors for L3 FEC prefix.
Total number of VC FEC processing errors	The total number of L3 VC FEC internal processing errors.
Total number of FECs	The total number of VC FECs.
Peer LDP ID	The remote LDP ID of the peer (or local LSR) from where the VC FEC originates.
VC-ID	The VC identifier associated with the VC FEC.
VC-Type	The VC Type associated with the VC FEC.
FEC-Type	The number that identifies the FEC type. The FEC type for VC FEC can be 128 or 129.
FEC_CB	Memory address of the FEC CB.
Idx	A monotonically increasing number assigned to each FEC in the LDP FEC tree.
Pend_notif	Any notification pending on this FEC.
UM Dist. done	Specifies when Upstream Mapping Distribution is complete.
Grp_id	Group identifier associated with the VC FEC.
Local-mtu	The local MTU for a specified VC FEC.
Remote-mtu	The remote MTU for a specified VC FEC.
MTU enforcement	The user configured MTU enforcement setting that display 'Enabled' when a specified VC ID is UP.
Label	MPLS label advertised to the upstream LDP LSR.

Examples

The following example displays the output of the **show mpls ldp fec prefix** command.

```
device# show mpls ldp fec prefix
Total number of prefix FECs: 4
Total number of prefix FECs installed: 1
Total number of prefix FECs filtered(in/out): 1/0
Total number of prefix FECs with LWD timer running: 0

Destination         State        Out-intf        Next-hop     Ingress   Egress   Filtered   LWD
77.77.77.77/32      current      --              --           No        Yes      -          No
144.144.1.1/32      current      e1/5            5.5.5.6      Yes       No       -          No
                                 e1/6            6.6.6.6
144.144.1.64/32     current      e1/5            5.5.5.6      Yes       No       IN         No
                                 e1/6            6.6.6.6
155.0.0.0/8         current      e1/3            3.3.3.5      Yes       No       -          No
```

The following example shows the output of the **show mpls ldp fec prefix-filter** command.

```
device(config)# ip prefix-list listabc deny 172.16.0.0/16 ge 24 le 24
device(config)# ip prefix-list listabc permit 172.16.0.0/16 ge 28 le 28
device(config)# ip prefix-list listabc per 0.0.0.0/0 ge 32 le 32
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# filter-fec list abc in
device(config)# show mpls ldp fec prefix filtered
Total number of prefix FECs: 11
Destination       State      Out-intf   Next-hop    Ingress   Egress  Filtered   LWD
77.77.77.77/32    current    --         --          No        Yes     -          No
144.144.1.1/32    current    e1/5       5.5.5.6     Yes       No      -          No
                             e1/6       6.6.6.6
144.144.1.64/32   current    e1/5       5.5.5.6     Yes       No      In         No
                             e1/6       6.6.6.6
155.0.0.0/8       current    e1/3       3.3.3.5     Yes       No      -          No
                             e1/4       4.4.4.5

device(config)#
device(config)# show mpls ldp fec prefix prefix-filter 172.16.8.0/24
FEC_CB: 0x2cd83d78, idx: 4, type: 2, pend_notif: None, fec_definition:22080000
State: current, Ingr: Yes, Egr: No, UM Dist. done: No
Prefix: 172.16.8.0/24
next_hop: 10.55.55.14, out_if: e3/16
Downstream mappings:
Local         LDP ID        Peer  LDP ID   Label State CB
10.44.44.44:0 10.14.14.14:0 1024  Retained (f)
```

The following example shows the output of the **show mpls ldp fec summary** command.

```
device# show mpls ldp fec summary
LDP FEC summary:
 Total number of prefix FECs: 8
 Total number of VC-FEC type 128:0
 Total number of VC-FEC type 129:0
LDP error statistics:
 Total number of route updates processing errors:0
 Total number of VC FEC processing errors: 0
```

The following example shows the output of the **show mpls ldp fec vc** command.

```
device# show mpls ldp fec vc

Total number of VC FECs:2
Peer LDP ID    State   VC-ID VC-Type FEC-Type Ingress Egress
10.125.125.1:0 current 100   4       128      Yes     Yes
10.125.125.1:0 current 1000  5       128      Yes     Yes
```

The following example shows the output of a MTU mismatch for VC ID of 100, where the VC label received from the remote peer is in a 'Retained' state instead of an 'Installed' state.

```
device# show mpls ldp fec vc 100
FEC_CB: 0x293916f8, inx:3, type:128, pend_notif:None
 State:current, Ingr:Yes, Egr:Yes, UM Dist. done:Yes
 VC_Id:100, vc-type:4, grp_id:0
 Local-mtu:2000, remote-mtu:1500, MTU enforcement:enabled

 Downstream mappings:
 Local LDP ID     Peer LDP Id     Label   State     CB
 10.128.128.28:0  10.125.125.1:0  800000  Retained  0x29391328(-1)

 Upstream mappings:
 Local LDP ID     Peer LDP ID     Label             CB
 10.128.128.28:0  10.125.125.1:0  800001            0x29391604(-1)
```

History

Release	Command history
5.4.00	This command was introduced.
5.5.00	This command was modified to display label withdrawal delay information.
5.6.00	The filtered options on the **show mpls ldp fec filtered** command now includes lists for both inbound and outbound FECs.
5.8.00	This command was modified to display the prefix FECs in order of the FEC definition.

show mpls ldp interface

Displays information about the LDP-enabled interfaces on the LSR.

Syntax

show mpls ldp interface [*intf_name* |**brief** | **ethernet** *slot/port* | **pos** *slot/port* | **tunnel** *tunnel_id* | **ve** *interface_id*]

Parameters

intf_name
Displays the selected interface information.

brief
Displays brief interface information.

ethernet *slot/port*
Displays the specified ethernet port.

pos *slot/port*
Displays the specified pos interface.

tunnel *tunnel_id*
Displays the specified tunnel.

ve *interface_id*
Displays the specified virtual ethernet interface.

Modes

EXEC mode.

Usage Guidelines

Command Output

The **show mpls ldp interface** command displays the following information:

Output field	Description
Label-space ID	The label space ID. The second two octets are always zero (0) for LSRs that use per-platform label spaces.
Nbr Count	The number of LDP peers or adjacencies that have been established on this interface. This number can be greater than one (1) when this is a multi-access network.
Hello Interval	The number of seconds between LDP Hello messages.
Next Hello	The number of seconds before the next LDP Hello message is sent (multicast) to the LDP interface (non-targeted). The LDP Hello message is unicast for a targeted interface. For every neighbor, the next LDP Hello message is sent at a different time. In order to find

Output field	Description
	out when the next LDP Hello message is sent out of any targeted adjacency, use the command **show mpls ldp neighbor.**

Examples

The following example shows the **show mpls ldp interface** command.

```
device# show mpls ldp interface
               Label-space   Nbr     Hello      Next
Interface      ID            Count   Interval   Hello
e4/1           0             1       5          0 sec
(targeted)     0             0       15         --
(targeted)     0             0       0          --
```

The following example show the interface transport address in use.

```
device #show mpls ldp interface
Total number of LDP interfaces : 3
                   Label-space    Nbr            Hello          Next      Interface
Interface          ID             Count          Interval       Hello     Transport Addr
e1/1               0              1              5              0 sec     YES
e1/2               0              1              5              0 sec     YES
e4/7               0              0              5              3 sec     NO
```

The following example show the interface transport address in use by the selected Ethernet slot and port.

```
device# show mpls ldp interface ethernet 1/1
e1/1, label-space ID: 0
  Nbr count: 1
  Hello interval: 5 sec, next hello: 3 sec
  Hello timeout: 15 sec
  Interface Transport address: in-use
```

History

Release version	Command history
6.1.00	This command was modified to show when the interface transport address is in use.

show mpls ldp neighbor

Displays information about the connection between this LSP and its LDP-enabled neighbors.

Syntax

show mpls ldp neighbor [*ip_addr space_id* | **detail** [*ip_addr* | *space_id*]]

Parameters

ip_addr

Displays the peer IP address.

space_id

The label space identifier.

detail

Displays detailed information.

ip_addr

The LDP identifier of the neighbor whose details are to be shown.

space_id

The label space identifier of the peer. If not provided, global (0) is assumed.

Modes

User EXEC mode

Usage Guidelines

show mpls ldp neighbordetail

This command operates in all modes.

Command Output

The **show mpls ldp neighbor detail** command displays the following information:

Output field	Description
Nbr Transport	The transport address of the LDP neighbor.
Interface	The interface to which the LDP neighbor is connected. "Targeted" indicates that the session between this device and the neighbor was established using Targeted Hello messages (that is, through extended discovery).
Nbr LDP ID	The neighbor's LDP identifier.
MaxHold	The number of seconds the device waits for its LDP peers to send a Hello message.
Time Left	The amount of time, in seconds, before the LDP neighbor times out when no Hello message is received from the neighbor.
Up Time	The Up Time is the time since the LDP adjacency is established. It is displayed in days, hours, minutes, and seconds. When there is no adjacency, then nothing is displayed.

Examples

The following example shows the output of the **show mpls ldp neighbor detail** command.

```
device# show mpls ldp neighbor detail
Nbr Transport Addr: 10.22.22.1, Interface: e1/1, Nbr LDP ID: 10.22.22.1:0
 MaxHold: 44 sec, Time Left: 43 sec, Up Time: 36 min 22 sec
Nbr Transport Addr: 10.22.22.1, Interface: e1/2, Nbr LDP ID: 10.22.22.1:0
 MaxHold: 75 sec, Time Left: 74 sec, Up Time: 36 min 27 sec
Nbr transport Addr: 10.33.33.1, Interface: 31/3, Nbr LDp ID: 10.33.33.1:0
 MaxHold: 75 sec, Time Left: 72 sec, Up Time: 36 min 22 sec
Nbr Transport Addr: 10.33.33.1, Interface: targeted, Nbr LDP ID: 10.33.33.1:0
 MaxHold: 75 sec, Time Left: 69 sec, Up Time: 35 min 36 sec
```

History

Release version	Command history
5.4.00	This command was modified. New variables were introduced under the **detail** option of the command.

show mpls ldp path

Displays information about active LDP-created LSPs for which the device is an ingress, transit, or egress LSR.

Syntax

show mpls ldp path *ip_prefix*

Parameters

ip_prefix

Designates the IP prefix to display.

Modes

User EXEC mode

Usage Guidelines

show mpls ldp path

The output of this command indicates that the device has received a label for the destination IP prefix (that is, the attached route) from the downstream peer and then advertised a label for that IP prefix to the upstream peer.

This command operates in all modes.

Command Output

The **show mpls ldp path** command displays the following information:

Output field	Description
Upstr-session (label)	The LDP identifier of the upstream peer, as well as the incoming label. Note that upstream session information does not apply to LSPs for which this is the ingress LER. Because the device uses a per-platform label space, the incoming interface for LDP-created LSP is not relevant.
Downstr-session (label, intf)	The LDP identifier of the downstream peer, as well as the outgoing label and interface. When applicable, the ingress interface 'intf' field displays a VE interface specified by the *vid* variable. Because the device uses a per-platform label space, the incoming interface for LDP-created LSP is not relevant. Note that downstream session information does not apply to LSPs for which this is the egress LER. When LDP selects its outgoing interface as an RSVP tunnel, the ingress interface 'intf' field displays the RSVP tunnel name.
Destination route	The destination route bound to this LSP.

Examples

The following example shows the output of the **show mpls ldp path** command.

```
device(config)# show mpls ldp path
Upstr-session(label)     Downstr-session(label, intf)    Destination route
10.3.3.3:0(3)            (egress)                        10.1.1.1/32
10.2.2.2:0(3)            (egress)                        10.1.1.1/32
10.3.3.3:0(1024)         10.2.2.2:0(3, e2/10)            10.2.2.2/32
10.2.2.2:0(1024)         10.2.2.2:0(3, e2/10)            10.2.2.2/32
(ingress)                10.2.2.2:0(3, e2/10)            10.2.2.2/32
10.3.3.3:0(1026)         10.3.3.3:0(3, e2/20)            10.3.3.3/32
10.2.2.2:0(1026)         10.3.3.3:0(3, e2/20)            10.3.3.3/32
(ingress)                10.3.3.3:0(3, e2/20)            10.3.3.3/32
```

show mpls ldp peer

Displays LDP peering information for each LDP session.

Syntax

show mpls ldp peer [[*peer-ip-addr label-id*] | **brief** | **detail**]

Parameters

peer-ip-addr label-id

Displays the peer IP address and the peer label space identifier.

brief

Displays summary LDP peering information.

detail

Displays detailed LDP peering information.

Modes

User EXEC mode

Usage Guidelines

Use this command to view summary or detailed information about LDP sessions and peers. This command operates in all modes.

Command Output

The **show mpls ldp peer** command displays the following information:

Output field	Description
Peer LDP ID	The LDP identifier of the peer LSR. The first four octets identify the peer LSR Ip address; the second two octets identify a label soace on the LSR. For LSRs that use per-platform label spaces, the second two octets are always zero (0).
Local LDP ID	This LSRs LDP identifier.
State	The LDP session state, as defined in *RFC 3036* . This can be 'Nonexistent', 'Initialized', 'OpenRec', or 'Operational'.
Session Status	Whether the session is operationally IP or DOWN.
Entity Idx	This displays the LDP session entity CB index maintained by the LDP session controller.
Targeted	Whether the session was established using Targeted Hello messages (that is, through extended discovery).
Target Adj Added	Whether the targeted adjacency was initiated for this LDP peer.
Num VLL	Number of VLL instances using the LDP peer.
Num VPLS	Number of VPLS instances using the LDP peer.
Rcvd VC FECs	Displays the contents of received VC FECs.

Output field	Description
From	Peer LSR ID where the VC FEC was received from.
VC ID	The VC identifier associated with the VC FEC.
Grp_Id	The group identifier associated with the VC FEC.
VC Type	The VC Type associated with the VC FEC.
MTU	The MTU value received in a VC Label Matching message from a peer.

Examples

The following example displays output of the **show mpls ldp peer** command.

```
device# show mpls ldp peer
Peer LDP ID     State         Num- VLL     Num-VPLS-Peer
10.2.2.2:0      Operational   2            0
10.3.3.3:0      Operational   0            0
10.8.8.8:0      Operational   2            0
10.9.9.9:0      Unknown       2            0
10.14.14.14:0   Operational   1            0
```

The following example displays output of the **show mpls ldp peer** with the **detail** keyword.

```
device# show mpls ldp peer detail
Peer LDP ID:10.2.2.2:0, Local LDP ID:10.1.1.1:0, State:Operational
Session Status UP, Entity Idx:4, Targeted:No, Target Adj Added:Yes
Num VLL:2, Num VPLS:0
Rcvd VC-FECs:
 From 10.2.2.2: Label:800001, VC Id:120, Grp_Id:0, VC Type:4, MTU:5000

Peer LDP ID:10.8.8.8:0, Local LDP ID:10.1.1.1:0, State:Operational
Session Status UP, Entity Idx:2, Targeted:Yes, Target Adj Added:Yes
Num VLL:2, Num VPLS:0
Rcvd VC-FECs:
 From 10.8.8.8: Label:16, VC Id:19, Grp_Id:0, VC Type:32773, MYU:5000
 From 10.8.8.8: Label:18, VC Id:18, Grp_Id:0, VC Type:32772, MTU:5555
```

show mpls ldp session

Displays information about LDP sessions between a specified router and VLL peers.

Syntax

show mpls ldp session [*ip_addr* | **brief** | **detail**]

Parameters

ip_addr

Displays LDP session information for the selected peer IP address.

brief

Displays summary LDP session information.

detail

Displays detailed LDP session information.

Modes

Privileged EXEC mode.

Usage Guidelines

Use this command with the **detail** option to display the number of FECs from the peer which are filtered due to the inbound FEC filter configuration.

Command Output

The **show mpls ldp session** command displays the following information:

Output field	Description
Peer LDP Ident	The VLL peer's LDP identifier, consisting of the LSR ID and the label space ID.
Local LDP Ident	The device's LDP identifier.
Active	Whether this LSR is playing an active role in session establishment.
State	The LDP session state, as defined in RFC 3036. Options are: • Nonexistent • Initialized • OpenRec • OpenSent • Operational
Adj	The type of adjacency formed with a peer. Possible values: • Link • Targeted
Role	Possible values: • Active

Output field	Description
	• Passive
Next KeepAlive	The number of seconds after which a Hello message is sent to a peer.
Hold time left	The number of seconds after which a session can be terminated when a 'Hello' message is not received from a peer within its time.
KeepAlive interval	The frequency within which LDP Hell' messages are sent out.
Max hold time	the length of time the device waits for a Hello message from its peer before terminating the session.
Neighboring interfaces	The physical interfaces on which the adjacency to the neighbor is formed.
TCP connection, state	The TCP local or remote IP address, port, and state.
Addresses bound to peer LDP Ident	IP addresses carried in the VLL peer's LDP address messages.
Next-hop addresses received from the peer	Next hop IP addresses received in the VLL peer's LDP address messages.

Examples

The following example displays the output of the show mpls ldp peer command. It displays information about LDP sessions between the device and VLL peers.

```
device# show mpls ldp session 14.14.14.14
Peer LDP ID: 14.14.14.14:0, Local LDP ID: 13.13.13.13:0, State: Operational
  Adj: Link, Role: Passive, Next keepalive: 0 sec, Hold time left: 30 sec
  Keepalive interval: 6 sec, Max hold time: 36 sec
  Local keepalive timeout: 36 sec
  Peer proposed keepalive timeout: 36 sec
  Up time: 3 hr 26 min 35 sec
  Neighboring interfaces: e2/1
  TCP connection: 13.13.13.13:646--13.14.1.14:9007, State: ESTABLISHED Transport Address: Interface
  Next-hop addresses received from the peer:
    13.14.1.14  13.14.1.141  13.14.2.14  14.14.14.14  19.14.1.14
    19.14.2.14
  IGP Sync:
    Unrecognized Notification Capability: Local: Off, Remote: Off
    Local State: In-sync, RemoteState: -
    Rx label silence time: 1000 ms, Timer not running
  Graceful restart: disabled
  Number of FECs Received from peer: 1
  Number of FECs installed from peer: 1
  Number of FECs filtered for peer(in/out): 0/0
```

History

Release	Command history
6.1.00	The command was modified to include display information regarding the interface transport address.
5.6.00	The command was modified to add the **in** and **out** keywords to the **filtered** option.
5.5.00	The command output was modified to display the total number of link and targeted sessions in operational state.

show mpls ldp statistics

Displays packet statistics for packet types and packet errors.

Syntax

show mpls ldp statistic *ip_addr*

Parameters

ip_addr

Specifies the selected IP address.

Modes

EXEC mode.

Usage Guidelines

Command Output

The **show mpls ldp statistics** command displays the following information:

Output field	Description
PacketType	The type of LDP packet being counted.
Total	The number of packets of the type describe for the row, sent and received since the Brocade device came UP.
Since last clear	The number of packets of the type described in the row, sent and received, since issuing the last clear command.
Errors	The type of packet error being counted. These errors are associated with the received packets only.
Total	The number of errors of the type describe in the row, generated since the Brocade device came UP.
Since last clear	The number of errors of the type described in the row generated since issuing the last clear command.

Examples

The following example displays the **show mpls ldp statistics** command:

```
device# show mpls ldp statistics
                  Total            Since last clear
Packet type       Sent  Received   Sent   Received
 Link Hello       215   214        215    214
 Targeted Hello   138   110        138    110
 Init             1     1          1      1
 KeepAlive        16    18         16     18
 Notification     0     0          0      0
 Address          2     0          2      0
 AddressWithdraw  0     0          0      0
 LabelMapping     0     0          0      0
 LabelRequest     0     0          0      0
 LabelWithdraw    0     0          0      0
 LabelRelease     0     0          0      0
 LabelAbortReq    0     0          0      0

Errors                         Total    Since last clear
 Rcv pkt bad pdu length        0        0
 Rcv pkt bad msg legnth        0        0
 Rcv pkt bad tlv length        0        0
 Rcv pkt notify unkn tlv       0        0
 Rcv pct notify unkn addrfam   0        0
 Rcv pkt missing tlv           0        0
 Rcv pkt incorrect tlv         0        0
 Rcv pkt malformed tlv         0        0
 Rcv pkt bad traffic parm      0        0
 Rcv pkt partial pdu           0        0
 Rcv pkt internal error        0        0
 TCP send error                0        0
 TCP get send pkt error        0        0
 TCP memory fail               0        0

Num of TCP socket buffers: 0
```

The following example displays the **show mpls ldp statistics** command for a specific session.

```
device# show mpls ldp statistics 10.10.10.10
Peer IP address:10.10.10.10
                   Total              Since last clear
Message Type       Sent   Received    Sent   Received
 Notify            0      0           0      0
 Hello Link        0      0           0      0
 Targeted Hello    0      0           0      0
 Initialize        1      1           1      1
 KeepAlive         11     11          11     11
 Addr              1      1           1      1
 AddrWdrw          0      0           0      0 LabelMap          1      1          1      1
 LabelReq          0      0           0      0
 LabelWdrw         0      0           0      0
 LabelRel          0      0           0      0
 LabelAbReq        0      0           0      0
 Unknown           0      0           0      0

Errors                         Total    Since last clear
 Rcv pkt bad pdu length        0        0
 Rcv pkt bad msg legnth        0        0
 Rcv pkt bad tlv length        0        0
 Rcv pkt notify unkn tlv       0        0
 Rcv pct notify unkn addrfam   0        0
 Rcv pkt missing tlv           0        0
 Rcv pkt incorrect tlv         0        0
 Rcv pkt malformed tlv         0        0
 Rcv pkt bad traffic parm      0        0
 Rcv pkt partial pdu           0        0
 Rcv pkt internal error        0        0
 TCP send error                0        0
 TCP get send pkt error        0        0
 TCP memory fail               0        0
Num of TCP socket buffers: 0
```

show mpls ldp tunnel

Displays the output sorted by the FEC address, which is the first column of the output.

show mpls ldp tunnel *ip_addr ip_mask* | **brief** | **detail** | **out-interface** [**ethernet** *slot/port* | **pos** *slot/port* | **ve** *interface_id*]

ip_addr

The tunnel destination IP address.

ip_mask

the tunnel IP prefix subnet mask.

brief

Displays brief information.

detail

Displays detailed information.

out-interface

Displays LDP tunnels going out of an interface.

ethernet *slot/port*

Displays the specified ethernet port.

pos *slot/port*

Displays the specified POS port.

ve *interface_id*

Displays the specified Virtual Ethernet (VE) interface.

EXEC mode.

The command displays information about LDP-created LSPs for which this device is the ingress LER.

The command is always sorted by FEC address.

This command operates in all modes.

The following example shows the command output sorted by the FEC address (the 'To' column).

```
Total number of LDP tunnels : 4
                Oper      Tunnel    Outbound
To              State     Intf      Intf
2.2.2.2         UP        tnl0      e1/1
2.2.2.3         UP        tnl4      e1/1
3.3.3.3         UP        tnl2      e1/1
20.1.1.1        UP        tnl1      e1/1
```

The following example displays the show mpls ldp tunnel command that includes the tunnel-index interface.

```
device#show mpls ldp tunnel 11.11.11.11
LDP tunnel tnl7, to 11.11.11.11/32
  Tunnel index: 7, metric: 0, status: UP
  Outgoing interface: e1/1, Next-hop index: 0
  Tunnel interface index: 18603
```

Release	Command History
5.4.00	This command is modified to include the new parameter **out-interface**.
5.5.00	The output of this command is modified to include all the paths in the LDP tunnel.
5.7.00	This command is modified so the output of the **show mpls ldp tunnel** command is always sorted by FEC address.
5.9.00	This command is modified to include the tunnel-interface index in the display output.

show mpls lsp

Displays information about configured and active dynamic *Multiprotocol Label Switching (MPLS) label-switched paths (LSPs)*.

Syntax

show mpls lsp autobw-sample | **brief** | **detail** | [**down** | **up** [**autobw-sample** | **detail** | **extensive** | **wide**]] | **extensive** | **name** *lsp_name* **autobw-sample** | **invalid-tunnel-interface wide** | **wide**

Parameters

auto-sample
Displays the sample History for all the auto-bandwidth LSPs.

brief
Displays brief information.

detail
Displays detailed information.

down
Displays operationally DOWN (inactive) LSPs.

up
Displays operationally UP (active) LSPs.

autobw-sample
Displays sample History.

detail
Displays detailed information.

extensive
Displays detailed information with History.

wide
Displays long LSP names.

name *lsp_name*
Displays information by the specified LSP name.

wide
Displays the long name of the LSP.

invalid-tunnel-interface
Displays LSPs that have an invalid tunnel-interface index because of a bad startup-configuration.

wide
Displays long LSP names.

Modes

EXEC mode.

Usage Guidelines

This command operates in all modes.

The **show mpls lsp brief** command displays the same information as the **show mpls lsp** command.

Command Output

The **show mpls lsp extensive** command displays the following information:

Output field	Description
Name	The name of the LSP. LSPs display in alphabetical order.
To	The egress LER for the LSP.
From	The LSPs source address, configured with the from command. When a source IP address has not been specified for the LSP with the **from** command, and the LSP has not been enabled, then 'n/a' is displayed in the 'From' field.
admin	The administrative state of the LSP. Once the user activates the LSP with the **enable** command, the administrative state changes from DOWN to UP.
status	The operational state of the LSP. This field indicates whether the LSP has been established through signaling and is capable of having packets forwarded through it. When the status of the LSP is DOWN, the reason the LSP is down is shown in parentheses "( )". There may be a short after the user enables the LSP that the administrative state of the LSP is UP, but the status is DOWN. Once the LSP establishes through signaling, both the administrative state and the status is UP.
tunnel interface (primary path)	The MPLS tunnel interface port ID.
Times primary LSP goes up since enabled	The number of times the status of the LSPs primary path transitions from DOWN to UP.
Metric	The metric for the LSP configured with the metric command.
Maximum retries	The maximum number of attempts the ingress LER attempts to connect to the egress LER, set with the retry-limit command.
no. of retries	The number of attempts the ingress LER has made to connect to the egress LER.
Pri. path	The name of the primary path for this LSP and whether the path is currently active.
up	Displays if the primary path is UP.
active	Displays if the primary path is active.
Setup priority	The configured setup priority for the LSP.
hold priority	The configured hold priority for the LSP.
Max rate	The maximum rate of packets that can go through the LSP (in kbps), set with the **traffic-eng max-rate** command.
mean rate	The average rate of packets that can go through the LSP (in kbps), set with the **traffic-eng mean-rate** command.
max burst	The maximum size (in bytes) of the largest burst the LSP can send at the maximum rate, set with the **traffic-eng max-burst** command.
Auto-bandwidth template	Displays the named auto-bandwidth template configuration information for the path specified by the **show mpls config autobw-template** *template_name* command.
mode	Displays when the LSP is in monitor-only mode or monitor-and-signal mode. The default mode is monitor-and-signal.
adjustment interval	The configured adjustment interval in seconds. Default value: 86400 seconds; range: 300 -2592000 seconds.
adjustment threshold	The configured adjustment threshold percentage. Default percentage: 0; range: 0 - 100 percent.

Output field	Description
minimum bw	The configured minimum bandwidth. Default value: 0 kbps; range: 0 - 2147483647 kbps.
maximum bw	The configured maximum bandwidth. Default value: 2147483647 kbps; range: 0 - 2147483647 kbps.
overflow limit	Displays the configured overflow limit.
underflow limit	The number of samples which have below the threshold to trigger a premature adjustment. Default value: 0; range: 0 - 65535.
sample-record	The record of all events related to auto-bandwidth of an LSP.
Constraint-based routing enabled	Whether CSPF is in effect for the LSP.
Path calculated using constraint-based routing	Whether the explicit path used by the active path was calculated using the constraint-based routing.
Path calculated using interface constraint	Whether the explicit path used by the active path was calculated using the interface-constraint routing.
Path cost	The total cost of this path.
Tie breaking	The tie-breaking method CSPF uses to select a path from a group of equal-cost paths to the egress LER, set with the **tie-breaking** command.
hop limit	The maximum number of hops a path calculated by CSPF can have, set with the **hop-limit** command.
LDP tunneling enabled	If LDP tunneling is enabled, the line reads 'yes'. If it is not enabled, the line reads 'no'.
Soft preemption enabled	Soft preemption minimizes traffic disruptions and gracefully reroute the preempted LSPs.
Sec. path	The name of the secondary path for this LSP and whether the path is currently active.
active	Displays if the secondary path is active.
Hot-standby	Whether the secondary path is a hot-standby path.
status	The operational state of the secondary path.
Setup priority	The name of the secondary path for this LSP and whether the path is currently active.
hold priority	The configured hold priority for the LSP.
Max rate	The maximum rate of packets that can go through the LSP (in kbps), set with the **traffic-eng max-rate** command.
mean rate	The average rate of packets that can go through the LSP (in kbps), set with the **traffic-eng mean-rate** command.
max burst	The maximum size (in bytes) of the largest burst the LSP can send at the maximum rate, set with the **traffic-eng max-burst** command.
Auto-bandwidth template	Displays the named auto-bandwidth template configuration information for the path specified by the **show mpls config autobw-template** *template_name* command.
mode	Displays when the LSP is in monitor-only mode or monitor-and-signal mode. The default mode is monitor-and-signal.
adjustment interval	The configured adjustment interval in seconds. Default value: 86400 seconds; range: 300 -2592000 seconds.
adjustment threshold	The configured adjustment threshold percentage. Default percentage: 0; range: 0 - 100 percent.
minimum bw	The configured minimum bandwidth. Default value: 0 kbps; range: 0 - 2147483647 kbps.
maximum bw	The configured maximum bandwidth. Default value: 2147483647 kbps; range: 0 - 2147483647 kbps.
overflow limit	Displays the configured overflow limit value.
underflow limit	The number of samples which have fallen below the threshold to trigger a premature adjustment. Default value: 0; range: 0 - 65535.
sample record	The record of all events related to auto-bandwidth of an LSP.
Constraint-based routing enabled	Whether CSPF is in effect for the LSP.

Output field	Description
hop limit	The maximum number of hops a path calculated by CSPF can have, set with the **hop-limit** command.
Soft preemption enabled	Soft preemption minimizes traffic disruptions and gracefully reroute the preempted LSPs.
Active Path attributes:	
Tunnel interface	The MPLS tunnel interface port ID.
outbound interface	The outbound interface taken by the active path of the LSP. When the egress interface is a VE-enabled interface, the VE interface ID specified by the *vid* variable.
Tunnel-interface index	The value of the tunnel-interface index (configured or allocated).
Tunnel interface	Please note that this specifies the vif index. For example: tnl1 would mean a vif of 1.
tunnel instance	Source port of the LSP.
outbound label	The outbound label used by the active path of the LSP.
Auto-bandwidth running info. mode	Displays when the auto-bandwidth running information mode is in monitor-only mode or monitor-and-signal mode. The default mode is monitor-and-signal.
adjustment interval	The configured adjustment interval in seconds. Default value: 86400 seconds; range: 300 -2592000 seconds.
adjustment threshold	The configured adjustment threshold percentage. Default percentage: 0; range: 0 - 100 percent.
overflow limit	Displays the configured overflow limit value.
underflow limit	The number of samples which have to be below the threshold to trigger a premature adjustment.
minimum bw	The configured minimum bandwidth. Default value: 0 kbps; range: 0 - 2147483647 kbps.
maximum bw	The configured maximum bandwidth. Default value: 2147483647 kbps; range: 0 - 2147483647 kbps.
Samples collected	Number of samples collected so far in the current adjustment-interval.
max sampled bw	The maximum of the samples collected so far in the current adjustment-interval.
last sample	The last sampled-bandwidth.
Overflow-count	Displays the number of samples that have consecutively exceeded the adjust-threshold. When a sample does not exceed the threshold, the counter is reset.
Underflow-count	Displays when the actual traffic rate is much less than the reserved bandwidth.
Sample-record	Records the sample history.
Adjustment ignored	This consecutive number of times the adjustment was ignored due to any reason.
Recorded routes	The addresses recorded by the RECORD_ROUTE object during RSVP signaling.
Protection codes/Rtr Id flag	The Local out-interface information label and protection flags: P: Local N: Node B: Bandwidth I: InUse R: RtrID

Examples

The following example shows the output of the **show mpls lsp brief** command:

```
device# show mpls lsp
*: The LSP is taking a Secondary path
                Admin   Oper   Tunnel   Up/Dn   Retry   Active
Name    To      State   State  Intl     Times   No.     Path
t1      10.3.3.3  UP      UP*    tnl1     1       5       v2
```

The following example shows the output of the **show mpls lsp detail** command:

```
device(config-mpls)#show mpls lsp detail
LSP c2, to 3.3.3.3, tunnel-interface index: 100
  From: 120.120.120.2, admin: UP, status: DOWN (CSPF fails: code 0)
  Times primary LSP goes up since enabled: 0
  Metric: 0
  Maximum retries: NONE, no. of retries: 0
  Pri. path: NONE, up: no, active: no
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  CSPF-computation-mode configured: use te-metric(global)
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: no
   Path calculated using interface constraint: no
  Tie breaking: random, hop limit: 0
  LDP tunneling enabled: no
  Soft preemption enabled: no
  Active Path attributes:
   Tunnel interface: tnl1, outbound interface: e1/6
   Tunnel index: 1, Tunnel instance: 1 outbound label: 3
   Recorded routes:
    Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
    6.6.6.41
```

The following example shows the output of the **show mpls lsp extensive** command:

```
device# show mpls lsp extensive
LSP lsp1, to 23.23.23.23
  From: 34.34.34.34, admin: UP, status: UP, tunnel interface(primary path): tnl1
  Times primary LSP goes up since enabled: 1
  Metric: 0, Adaptive
  Maximum retries: NONE, no. of retries: 0
  Pri. path: NONE, up: yes, active: yes
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  Auto-bandwidth. template: template1, mode: monitor-only
    adjustment interval: 86400 sec, adjustment threshold: 0
    minimum bw: 0 kbps, maximum bw: 2147483647 kbps
    overflow limit: 0, underflow limit: 20, sample-record: disabled
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: yes
   Path calculated using interface constraint: no
   Path cost: 20
  Tie breaking: random, hop limit: 0
  LDP tunneling enabled: no
  Soft preemption enabled: no
  Sec. path: via16, active: no
   Hot-standby: no, status: down, adaptive
   Setup priority: 7, hold priority: 0
   Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
   Auto-bandwidth. template: NONE, mode: monitor-and-signal
    adjustment interval: 300 sec, adjustment threshold: Table
    minimum bw: 0 kbps, maximum bw: 2147483647 kbps
    overflow limit: 5, underflow-limit: 10, sample-record: enabled
   Constraint-based routing enabled: yes
   hop limit: 0
   Soft preemption enabled: no
  Active Path attributes:
   Tunnel interface: tnl1, outbound interface: e4/3
   Tunnel index: 2, Tunnel instance: 1 outbound label: 2049
   Auto-bandwidth running info. Mode: monitor-only
    adjustment interval: 1200 sec(T), adjustment threshold: Table(T)
    overflow limit: 0, underflow limit: 3
    minimum bw: 0 kbps(T), maximum bw: 9647 kbps(T)
    Samples collected: 14, max sampled bw: 0 kbps, last sample: 0 kbps
    Overflow-count: 0, Underflow-count: 2,max-underflow-sample: 34kbps
    Sample-record: enabled(T)
    adjustment due in 1174 seconds
    Adjustment ignored: 0 time(s)
    No adjustment since activation. Current bandwidth: 0 kbps
   Recorded routes:
    Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
    31.31.31.16 -> 161.161.161.1
```

The following example shows the output of the **show mpls lsp wide** command. The full LSP name displays on a single line.

```
device# show mpls lsp wide
note: LSPs marked with * are taking a Secondary Path
                  Admin  Oper  Tunnel  Up/Dn  Retry  Active
Name     To       State  State Intl    Times  No.    Path
tunnel1  10.3.3.3  UP     UP    tnl0    1      0      --
tunnel2  10.3.3.3  UP     UP    tnl4    1      0      ppath1
tunnelfromsanfranciscotonewyork
         10.3.3.3  UP     UP    tnl3    1      0      pathfrom sanfranciscotonewyork
```

The following example shows the bandwidth inherited from the protected LSP.

```
device# show mpls lsp name to_NY
LSP to_NY, to 28.28.28.28
From: 34.34.34.34, admin: UP, status: UP, tunnel interface(primary path): tnl8
Times primary LSP goes up since enabled: 1
Metric: 0
Maximum retries: NONE, no. of retries: 0
Pri. path: to-NY_via_Chicago, up: yes, active: yes
Setup priority: 7, hold priority: 0
Max rate: 0 kbps, mean rate: 2000 kbps, max burst: 0 bytes
CSPF-computation-mode configured: use te-metric(global)
Constraint-based routing enabled: yes
Path calculated using constraint-based routing: yes
Path calculated using interface constraint: no
Path calculated using te-metric
Path cost: 22
Tie breaking: random, hop limit: 0
LDP tunneling enabled: no
Soft preemption enabled: no
Active Path attributes:
Tunnel interface: tnl8, outbound interface: ve11
Tunnel index: 4, Tunnel instance: 1 outbound label: 2048
Explicit path hop count: 3
150.150.150.16 (S) -> 93.93.93.9 (S) -> 28.28.28.28 (L)
Recorded routes:
Protection codes/Rtr Id flag: P: Local N: Node B: Bandwidth I: InUse R: RtrId
150.150.150.16 (PN) -> 93.93.93.9 (P) -> 90.90.90.10
Fast Reroute: facility backup desired, node protection desired
Bandwidth: 2000 kbps (Inherited from Protected LSP)
Backup LSP: UP, out-label: 2048, outbound interface: e1/9 bypass_lsp: to_NY_via_DC
cost: 0
cspf-group computation-mode: disabled
cspf-computation-mode use-bypass-metric: disabled
FRR Forwarding State: Pri(active), Backup(up)
```

History

Release version	Command history
5.4.00	This command is modified to include new events that are logged in the LSP history. The only change is that a new message has been defined for an RRO change. The rest of the fields are unchanged.
5.5.00	This command is modified to include LSP history with IGP synchronization related history logs when using the extensive option.
5.6.00	This command is modified to show: • The **underflow-limit** parameter and the number of consecutive under-flows. • The **adjustment-threshold** is used from the global mode and is indicated by the value of the current rate. • The sample history for the current adjustment interval. • The **autobw-sample** parameter is introduced.
5.8.00	This command is modified to include "Inherited from Protected LSP" in display output for the **detail**, **extensive**, and **wide** options.
5.9.00	This command is modified so the output of **show mpls lsp** command in the non-brief versions includes the tunnel-interface index. This command is modified to include an option to display those LSPs that have invalid tunnel-interface index because of bad startup-configuration (**invalid-tunnel-interface**).

show mpls lsp_p2mp_xc

Displays hardware information about the forwarding information of hardware that is allocated for the *point-to-multipoint (P2MP)* cross-connect.

Syntax

show mpls lsp_p2mp_xc *in_label*

Parameters

in_label

Specifies the MPLS input label value.

Modes

Privileged EXEC mode.

Usage Guidelines

The **show mpls lsp_p2mp_xc** command displays information about the forwarding information of hardware that is allocated for the *point-to-multipoint (P2MP)* cross-connect.

This command operates in all modes.

Examples

The following example displays hardware forwarding statistics on a Brocade NetIron MLX Series device:

```
device# show mpls lsp_p2mp_xc
P2MP XC TABLE:
TOTAL USED = 2
         IN-LABEL  XC#  FID     MVID  IN-PORT   NUM_OUT_SEGS
         1159      0    0a00a   106   65535     1
         1160      1    0a00b   107   65535     1

device# show mpls lsp_p2mp_xc 1159
TOTAL OUT_SEGS under the given in_label = 1
         BRANCH-ID OUT-LABEL OUT-PORT    NH-ID
         0         0         14          6
        Event History -
         Tue Aug 14 02:21:54 2012 P2MP BRANCH ADD
         Tue Aug 14 02:21:54 2012 P2MP XC ADD
flag: 0, pool_index:1, avail_data:270e0800
```

The following example displays hardware forwarding statistics on a Brocade NetIron CES Series device:

```
device# show mpls lsp_p2mp_xc
P2MP XC TABLE:
TOTAL USED = 1
 IN-LABEL  XC# IP-TTI @ PPCR{1, 2, 3} MPLS-TTI@{PPCR 1, 2, 3} IN-PORT NUM_OUT_SEGS START-DIT
 1024      1   65274                 65275                    1/1     2            2049

device# show mpls lsp_p2mp_xc 1024
TOTAL OUT_SEGS under the given in_label = 2
         BRANCH-ID OUT-LABEL OUT-PORT    NH-ID      DIT      TSI
         0         2001      4           0          2049     0
         1         2002      4           0          2050     1
        Event History -
         Tue Aug 14 12:53:17 2012 P2MP BRANCH ADD
         Tue Aug 14 12:52:33 2012 P2MP BRANCH ADD
         Tue Aug 14 12:52:33 2012 P2MP XC ADD
```

History

Release	Command history
5.5.00	This command is introduced.

show mpls path

Displays a list of device hops that specifies a route across an MPLS domain.

Syntax

show mpls path [*path_name* | **detail** | **wide**]

Parameters

path_name

Displays only information for a specified path.

wide

Displays the full path name on a single line.

detail

Displays detailed path information.

Modes

Usage Guidelines

A path is a list of device hops that a specifies a route across an MPLS domain. The user can create a path, and then configure LSPs that see the path. When the LSP is enabled, the ingress LER attempts to signal the other LSRs in the path, so that resources can be allocated to the LSP.

This command operates in all modes.

Command Output

The **show mpls path** command displays the following information:

Output field	Description
Path name	The configured name of the path.
Address	The IP address of each node in the path. A node corresponds to an MPLS-enabled router in the network.
Strict or Loose	Whether the node is strict or loose. A strict node means that the router must directly connect to the preceding node. A loose node means that the other routers can reside between the source and destination nodes.
Usage Count	The number of LSPs that are either currently using or configured to use the path. For example, when an LSP named 'to_sqa' has primary and secondary paths and both paths are configured to use the same MPLS path 'path_to_sqa', then the usage count for 'path_to_sqa' would be two (when no other LSP in the system is configured to use 'path_to_sqa'.

Examples

The following example displays the output of the **show mpls path** command.

```
device# show mpls path
Path Name   Address       Strict/loose   Usage Count
to110_120   10.110.110.2  Strict         1
            10.120.120.3  Strict
to2_pri     10.10.10.2    Strict         0
to2_sec     10.110.110.2  Strict         0
to3         10.110.110.2  Loose          1
            10.120.120.3  Loose
to3_pri     10.10.10.2    Strict         1
            10.120.120.3  Strict
to3_sec     10.110.110.2  Strict         0
            10.120.120.3  Strict
to4         10.110.110.2  Loose          1
            10.120.120.3  Loose
            10.130.130.4  Loose
to_23       10.110.110.2  Strict         1
            10.20.20.3    Strict
```

The following example displays the **show mpls path wide** command. This option lets the full name of the display on a single line.

```
device# show mpls path wide
Path Name   Address       Strict/loose   Usage Count
pathfromsanfranciscotonewyork
            10.10.10.2    Strict         1
ppath       10.10.10.2    Strict         1
spath       10.20.20.2    Strict         1
```

History

Release version	Command history
4.1.00	This command is modified, so the display output displays additional information.
5.1.00	This command is modified so when using the **wide** option; the LSP name is displays on a single line. Previously, an LSP name greater than 12 characters was wrapped to multiple lines.

show mpls policy

Displays the current parameter settings configured under the MPLS policy mode.

Syntax

show mpls policy

Modes

MPLS policy configuration mode

Usage Guidelines

The output includes a display of bypass liberal mode if the **use bypass liberal** keyword was configured as part of the **CSPF computation-mode** command.

Command Output

The **show mpls policy** command displays the following information:

Output field	Description
Current MPLS policy settings:	
CSPF interface constraint	Directs the router to include the interface address as a constraint when it determines the shortest path.
CSPF-Group computation-mode	Specifies the mode that is used when setting up a fate-sharing group.
CSPF computation-mode :	
Use bypass metric	Displays if enabled or disabled. TE metric of TE link for CSPF computation.
Use bypass liberal	Displays if enabled or disabled. Liberal mode for CSPF facility backup computation.
Use te-metric	Displays if enabled or disabled. By default, the cspf-computation mode is set to use te-metric.
ignore-overload-bit	Displays if enabled or disabled. • With this enabled, even when overload bit is set on a transit a router, CSPF at the ingress will not reject any path for new LSPs. • If the ignore overload bit is set, already existing transit sessions will not be brought down from ingress on enabling overload bit on transit router.
TTL propagation for MPLS label	Displays if the TTL propagation for MPLS is enabled or disabled.
IPVPN	Displays if IPVPN is enabled or disabled.
IP over MPLS	Displays ID IP over MPLS is enabled or disabled.
Inter-AS-route filtering	When the user enables inter-AS-route filtering, the RTM does not send any inter-AS routes to MPLS.
Intra-AS iBGP route filtering	Displays if intra-AS iBGP route filtering is enabled or disabled.
Ingress tunnel accounting	Displays if ingress tunnel accounting is enabled or disabled.
Polling interval for MPLS LSP traffic statistics	Displays the polling interval, in seconds.
Advertise TE parameters via	Displays which level option enables LSPs with TE extensions. The level-1 option enables TE extensions for the IS-IS level-1 domain. The level-2 option enables LSPs with TE extensions for the IS-IS level-2 domains.

Output field	Description
Handle IGP neighbor down event - ISIS	Displays if IS-IS is handling the IGP neighbor DOWN event.
Handle IGP neighbor down event - OSPF	Displays if OSPF is handling the IGP neighbor DOWN event.
LSP rapid retry	Displays if LSP rapid retry is enabled or disabled.
Maximum number of retries	Displays the maximum number of times the port will try the health check. Values are from 3 - 64. The default value is 7.
LSP periodic retry time	Displays the LSP periodic retry time in seconds.
FRR backup/detour retry time	Displays the FRR backup and detour retry time in seconds.
Auto-bandwidth	Displays if auto-bandwidth is enabled or disabled.
Sample-interval	On changing the sample-interval the sample-timer is reset for all the auto-bandwidth LSPs. Any rate information already collected so far in the current sample-interval is considered a valid sample.
Maximum samples recorded per LSP	Displays the maximum samples recorded per LSP.
Soft preemption cleanup-timer	Interval time between when the path is taken down and the new LSP is established. Any traffic attempting to use the LSP is lost.
MPLS TE Periodic Flooding Timer	Displays the timer in seconds. All MPLS interfaces are checked every three minutes by default. TE advertisements are triggered when there is a difference in the available bandwidth and advertised available bandwidth.
MPLS TE flooding thresholds:	
Global UP thresholds	Displays global UP thresholds. UP values are 10, 20, 30, 40, 50, 55, 60, 65, 70, 85, 90, 92, 93, 94, 95, 96, 97, 98, 99, 100.
Global DOWN thresholds	Displays global DOWN thresholds. DOWN values are 99, 98, 97, 96, 95, 94, 93, 92, 91, 90, 85, 80, 75, 70, 65, 60, 55, 50, 45, 30, 20, 10.
Default UP thresholds	Displays default UP thresholds. UP values are 10, 20, 30, 40, 50, 55, 60, 65, 70, 75, 80, 85, 90, 92, 93, 94, 95, 96, 97, 98, 99, 100.
Default DOWN thresholds	Displays default Down thresholds. DOWN values are 99, 98, 97, 96, 95, 94, 93, 92, 91, 90, 85, 80, 75, 70, 65, 60, 55, 50, 40, 30, 20, 10.

Examples

The following example displays the output of the **show mpls policy** command:

```
device# show mpls policy
Current MPLS policy settings:
  CSPF interface constraint: disabled
  CSPF-Group computation-mode: disabled
   Use bypass metric: disabled
   Use bypass liberal: disabled
   Use te-metric  (default), Ignore-overload-bit: disabled
  TTL propagation for MPLS label: disabled, IPVPN: disabled, IP over MPLS: enabled
  Inter-AS route filtering: enabled, Intra-AS iBGP route filtering: disabled
  Ingress tunnel accounting: disabled
  Polling interval for MPLS LSP traffic statistics: 300 seconds
  Advertise TE parameters via: OSPF
  Handle IGP neighbor down event - ISIS: No OSPF: No
  LSP rapid retry: enabled, maximum number of retries: no limit
  LSP periodic retry time: 30 seconds
  FRR backup/detour retry time: 30 seconds
  Auto-bandwidth: enabled, sample-interval: 60 seconds
   Maximum samples recorded per LSP: 1500
  Soft preemption cleanup-timer: 30 seconds
  MPLS TE Periodic Flooding Timer : 180 seconds
  MPLS TE flooding thresholds
    Global  UP   thresholds : None
    Global  DOWN thresholds : None
    Default UP   thresholds : 15 30 45 60 75 80 85 90 95 96 97 98 99 100
    Default DOWN thresholds : 99 98 97 96 95 90 85 80 75 60 45 30 15
```

History

Release	Command history
5.6.00	This command was modified to include bypass liberal output when the **use bypass liberal** keyword is configured in the **cspf-computation-mode** command.
5.8.00	This command was modified to include 'CSPF computation-mode' information in the display output.

show mpls route

Displays the contents of the MPLS routing table.

Syntax

show mpls route [*ip_addr* [**/** *ip_mask*]]

Parameters

ip_addr

Specifies the destination IP address.

/ *ip-mask*

Specifies the IP subnet mask.

Modes

User EXEC mode

Usage Guidelines

With LDP ECMP LER tunnels, the output for one tunnel could be greater than one line where each line shows one outgoing path - the repetitive lines do not have the 'Destination' and 'Tnnl' columns filled because they match what is in the first line.

Command Output

The **show mpls route** command displays the following information:

Output field	Description
Destination	The destination for the route. This can be either the address of the egress LER in an LSP, or a configured alias.
Gateway	The address of the egress LER in the LSP. When the destination address is not a network alias, the gateway is the same as the destination address.
Tnnl	The address of the egress LER in the LSP. When the destination address is not a network alias, the gateway is the same as the destination address.
Port	The MPLS tunnel interface associated with the LSP. The port field displays whether an interface/port is an Ethernet port, POS port, or a VE interface. The VE interface ID is specified by the *vid* variable. When applicable, the egress interface of the routing entry displays the VE interface. The port display format for interface or port is as follows: • [e|p] slot or port • "e" represents an Ethernet port • "p" represents a POS port
Label	The MPLS label received from the downstream router.
Sig	The signal protocol type associated with the label. Possible values are: • L – LDP

Output field	Description
	• R – RSVP
Cost	The metric for the LSP, set with the metric command in the LSPs configuration.
Use	The number of LSPs that are either currently using or configured to use the path. For example, when an LSP named "to_sqa" has primary and secondary paths and both paths are configured to use the same MPLS path "path_to_sqa," then the usage count for "path_to_sqa" would be two (when no other LSP in the system is configured to use "path_to_sqa")."

Examples

The following example displays the **show mpls route** command.

```
device# show mpls route
Total number of MPLS tunnel routes: 4
R:RSVP L:LDP S:Static O:Others
  Destination     Gateway      Tnnl  Port  Label Sig Cost Use
1 10.12.12.12/32  10.12.12.12  tnl1  e2/1  3     R   0    0
2 10.12.12.12/32  10.12.12.12  tnl5  e2/1  3     L   0    0
                  10.12.12.12        e2/2  3     L   0    0
                  10.12.12.12        e3/8  3     L   0    0
3 10.13.13.13/32  10.13.13.13  tnl4  e1/1  3     L   0    0
4 10.77.77.12/32  10.12.12.12  tnl10 e2/1  3     L   0    0
                  10.12.12.12        e2/2  3     L   0    0
                  10.12.12.12        e3/8  3     L   0    0
```

History

Release	Command history
5.5.00	With LDP ECMP LER tunnels, the output for one tunnel could be greater than one line where each line shows one outgoing path.

show mpls rsvp interface

Displays the status of RSVP on devices where it is enabled.

Syntax

show mpls rsvp interface brief | **detail** | [**ethernet** | **pos** | **ve** *slot/port*]

Parameters

brief

Displays brief interface information.

detail

Displays detailed interface information.

ethernet *slot/port*

Displays the specified ethernet port.

pos *slot/port*

Displays the specified POS port.

ve *slot/port*

Displays the specified virtual ethernet interface.

Modes

Privileged EXEC mode.

Usage Guidelines

clear mpls rsvp statistics

This command operates in all modes.

Command Output

The **show mpls rsvp interface** command displays the following information:

Output field	Description
Status	Whether the interface is UP or DOWN.
MD5	Whether RSVP message authentication is enabled on the interface.
RelMsg	Whether RSVP reliable messaging is enabled on the interface.
Bundle	Whether RSVP bundle messages are enabled on the interface.
SRefresh	Whether RSVP summary refresh is enabled on the interface.
Num of OutSegAct/Inact/Resv	Out segments are traffic connections on the link. These connections may be active or inactive. 'Resv' represents the number of active out segments with a nonzero mean rate.
Num of Preempts	Number of times lower-priority LSPs have been preempted on this interface.

Examples

The following example displays the **show mpls rsvp interface** command:

```
device# show mpls rsvp interface

Interface      State  MD5  RelMsg  Bundle  SRefresh  Act/Inact/Resv  Preempts
e3/2 (Trunk8)  UP     OFF  ON      ON      ON        0/0/0           0
e3/4 (Trunk9)  Up     OFF  ON      ON      ON        0/0/0           0
e3/6           Up     OFF  ON      ON      ON        0/0/0           0
e3/7 (Trunk2)  Up     OFF  ON      ON      ON        1699/0/1684     1142
e3/8 (Trunk6)  Up     OFF  ON      ON      ON        167/0/106       0
e4/3 (Trunk3)  Up     OFF  ON      ON      ON        2526/0/2526     1471
e4/5 (Trunk4)  Up     OFF  ON      ON      ON        8421/0/8421     774
e7/1 (Trunk17) Up     OFF  ON      ON      ON        8480/0/8421     5479
e7/2 (Trunk19) Up     OFF  ON      ON      ON        7489/0/7484     0
e9/3 (Trunk7)  Up     OFF  ON      ON      ON        178/0/158       0
(output truncated)
```

The following example displays a shorter output, using the **show mpls rsvp interface brief** command.

```
device# show mpls rsvp interface brief
Interface    State    MD5 Auth
e2/1         Up       OFF
e2/2         Dn       OFF
e4/1         Dn       OFF
e4/2         Dn       OFF
```

show mpls rsvp neighbor

Displays RSVP neighbors that were discovered dynamically during the exchange of RSVP packets.

Syntax

show mpls rsvp neighbor [*ipv4address* | **detail**]

Parameters

ip_addr

Specifies the IP address of a learned neighbor.

detail

Displays RSVP neighbor information in a detailed format.

Modes

Privileged EXEC mode.

Usage Guidelines

Use this command to display all the current RSVP neighbors for this router.

The 'RR' and 'MsgID' flags in this command show the ability of the neighbor to support Refresh Reduction and Message IDs respectively.

The 'MsgID' field is set to 'YES' in the following cases:

- This field is defaulted to 'YES' initially.
- It is set to 'YES' if the neighbor sends a message containing a Message ID.
- It is also set to 'YES' if the remote MPLS interface is configured to send Message IDs to this neighbor.

The 'MsgID' field is set to 'NO' when the peer rejects a message (with a 'PathErr' or 'ResvErr') because it contains a Message ID object.

If the neighbor sends a NACK to a Message ID object that is sent and then subsequently sends a Path or Resv message that does not contain a Message ID, then RSVP sets this field to 'NO'. This allows RSVP to inter-operate with devices that do not support Message IDs.

This command operates in all modes.

Command Output

The **show mpls rsvp neighbor** command displays the following information:

Output field	Description
RSVP neighbors learnt	Number of neighbors the router has learned.
Nbr Address	Address of the learned neighbor.
Interface	Name of the interface where the neighbor has been detected.

Output field	Description
State	Current status of the neighbor. **UP** - Router can detect RSVP-TE Hello messages from the neighbor. **DOWN** - Router has received a failure from the neighbor or change in the sequence numbers in RSVP Hello messages sent by the neighbor.
Last_Change	Time elapsed since the neighbor state changed. Format: days: hours: minutes: seconds.
Number of LSPs to or from this Nbr	This field displays the number of LSPs or RSVP sessions using this next-hop (neighbor).(Detail mode only.)
Hello-interval	**Hello-interval** - Frequency at which RSVP-TE Hello Request messages are sent on the interface, in seconds.
Hello-tolerance	**Hello-tolerance** - The number of hello periods that may pass without receiving a complete Hello message before the Hello session times out. (Detail mode only.)
Hello Tx/Rx Count	Number of Hello packets sent to or received from the neighbor.
RR/MsgID Support	Indicates if Refresh Reduction and Message ID support is enabled and or supported by the neighbor. (**Y** - Enabled, **N** - Disabled)
No Hello message received since	This field displays how far back (in seconds) the last RSVP Hello (Request OR Ack) message was received.
Time left to send next Hello Req	This field is valid and displays the time only when the Neighbor supports RSVP Hellos. Otherwise, it displays "-". (Detail mode only.)
Remote instance	Identifier provided by the remote router during Hello messages (Dest_Instance or Neighbor_Src_Instance). (Detail mode only.)
Local instance	Identifier sends to the neighbor during Hello messages (Src_Instance). (Detail mode only.)
Refresh Reduction	Indicates if Refresh Reduction is enabled or supported by the neighbor. (Detail mode only.)
Message ID	Indicates if Message ID support is enabled by the neighbor. (Detail mode only.)

Examples

The following example displays the output of the **show mpls rsvp neighbor** command.

```
device# show mpls rsvp neighbor
RSVP neighbors learnt: 4
Nbr Address Interface State Last_Change HelloTx/Rx RR/MsgID
d:h:m:s Count Support
10.152.152.15 e1/2 UP 10:2:31:44 8498/8349 Y/Y
10.92.98.9 e1/12 UP 0:6:39:36 3995/3587 N/Y
10.31.31.15 e4/3 DOWN 6:6:39:36 3000/1267 N/Y
10.92.99.9 e3/2 UP 0:0:31:44 2995/0 N/N

device# show mpls rsvp neighbor 10.92.98.9
Nbr Address: 92.92.98.9, Interface: e1/12, State: UP
Last changed time (d:h:m:s): 0:6:39:38, Number of active LSPs to or from this
Nbr: 22
Hello sent: 3995, received: 3587, Hello-interval: 15 sec, Hello-tolerance: 5
No Hello message received since: 5 sec
Time left to send next Hello Req: 10 sec
Remote instance: 0x65c6b2, Local instance: 0x5a4f9f21
Refresh Reduction: Disabled, Message ID: Enabled

device# show mpls rsvp neighbor 10.1.1.1
RSVP neighbor with the provided IP address does not exist
```

History

Release	Command History
5.6.00	This command is introduced.

show mpls rsvp session

Displays information regarding *Resource reSerVation Protocol (RSVP)* sessions.

Syntax

show mpls rsvp session [**backup** | **brief** | **bypass** | **destination** | **detail** | **detour** | **down** | **egress** | **extensive** | **in-interface** | **ingress** | **name** *sess-name* | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** | **up** | **wide**]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

bypass
Displays bypass session.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name *sess-name*
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in soft preemption pending state.

transit
Displays a transit session.

up
Displays up session.

wide
Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

The **show mpls rsvp session brief** command displays the same information as the **show mpls rsvp session** command.

This command operates in any mode.

Command Output

The **show mpls rsvp session** command displays the following information:

Output field	Description	Command
Ingress RSVP	Displays information about ingress RSVP sessions.	**show mpls rsvp session** **show mpls rsvp session detail** show mpls rsvp session **extensive**
Transit RSVP	Displays information about transit RSVP sessions.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive**
Egress RSVP	Displays information about egress RSVP sessions.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive**
To	Destination (egress LER) of the session.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**
From	Source (ingress LER) of the session; the source address for the LSP configured with the **from** command.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**
St	State can be UP or DOWN.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**

Output field	Description	Command
Style	The RSVP reservation style. Possible values are *Fixed Filter (FF)*, *Wildcard Filter (WF)*, or *Shared Explicit (SE)*.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**
Lbl_In	The label for inbound packets on this LSP.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**
Lbl_Out	The label applied to outbound packets on this LSP.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**
Out_If	The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the *vid* variable.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**
LSPname	The name of the LSP.	**show mpls rsvp session** **show mpls rsvp session detail** **show mpls rsvp session extensive** **show mpls rsvp session wide**
Time left in seconds	The amount of time left for the PATH or RESV refreshes.	**show mpls rsvp session detail** **show mpls rsvp session extensive**
Tspec	Traffic engineering specification for the LSP, including the max-rate (“peak”), mean rate (“rate”), number of burst bytes (“size”), maximum policed unit (“M”—or maximum packet size), and minimum policed unit (“m”—or minimum packet size).	**show mpls rsvp session detail** **show mpls rsvp session extensive**
Explicit path hop count	The number of explicit hops used in this RSVP session.	**show mpls rsvp session detail** **show mpls rsvp session extensive**
Received RRO count	The number of Record Route Objects received on this RSVP session.	**show mpls rsvp session detail** **show mpls rsvp session extensive**
PATH sentto	Address of the next LSR in the LSP, and the interface used to reach this LSR. When applicable, ‘PATH sentto’ displays a VE interface specified by the *vid* variable.	**show mpls rsvp session detail** **show mpls rsvp session extensive**
PATH rcvfrom	Address of the previous LSR in the LSP, and the interface used to reach this LSR. When the session is downstream only, then it is displayed. When applicable, ‘PATH rcvfrom’ displays a VE interface specified by the *vid* variable.	**show mpls rsvp session detail** **show mpls rsvp session extensive**
PATH history	Displays history of the last 20 RSVP event. Each event contains: • Event index (used to provide the number of events). • Time stamp • File name and line number where the event is logged. • Event description and extra information associated with each event.	**show mpls rsvp session extensive**

Examples

The following example displays the **show mpls rsvp session** command.

```
device(config)# show mpls rsvp session
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Ingress RSVP: 10 session(s)
To          From             St Style Lbl_In Lbl_Out Out_If LSPname
10.22.22.22 10.11.11.11      Up FF    -      3       e4/3   xmr2
10.33.33.33 10.11.11.11(DI)  Up SE    -      3       e4/4   rj-vpls
10.33.33.33 10.11.11.11      Up SE    -      1039    e1/15  rj-vpls
..............

Transit RSVP: 1009 session(s)
To          From             St Style Lbl_In Lbl_Out Out_If LSPname
10.22.22.22 10.33.33.33      Up SE    1024   3       e4/3   2
10.22.22.22 10.33.33.33(DI)  Up SE    1072   1319    e2/4   toxmr2frr-
..............

Egress RSVP: 62 session(s)
To          From             St Style Lbl_In Lbl_Out Out_If LSPname
10.11.11.11 10.22.22.22(DE)  Up SE    3      -       -      toxm1-frr
10.11.11.11 210.22.22.22(DE) Up SE    3      -       -      toxm1-frr
10.11.11.11 10.22.22.22      Up SE    3      -       -      toxm1-frr
10.11.11.11 10.44.44.44      Up FF    3      -       -      toxmr1
```

The following command allows the user to display the full LSP name in a single line.

```
device# show mpls rsvp session wide
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Ingress RSVP: 4 session(s)
10.3.3.3 10.2.2.2        Up SE - 3 e1/1 tunnel1
10.3.3.3 10.10.10.10(BI) Dn -  - - e1/3 tunnel1
10.3.3.3 10.2.2.2(BYI)   Up SE - 3 e1/3 by1
10.3.3.3 10.2.2.2        Up SE - 3 e1/1 tunnelfromsanfranciscotonewyork
10.3.3.3 10.10.10.10(BI) Dn -  - - e1/3 tunnelfromsanfranciscotonewyork
10.3.3.3 10.2.2.2(BYI)   Up SE - 3 e1/3 bypasstunnelfromsfotonewyork

Transit RSVP: 0 session(s)
Egress RSVP: 0 session(s)
```

the following example displays the command using the wide parameter.

```
device# show mpls rsvp session backup wide
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress
Ingress RSVP: 2 session(s)
To        From            St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.3.3.3  10.2.2.2        Up  SE     -       3        e1/1    tunnel1
10.3.3.3  10.10.10.10(BI) Dn  -      -       -        e1/3    tunnel1
10.3.3.3  10.2.2.2        Up  SE     -       3        e1/1    tunnelfromsanfranciscotonewyork
10.3.3.3  10.10.10.10(BI) Dn  -      -       -        e1/3    tunnelfromsanfranciscotonewyork
Transit RSVP: 0 session(s)
Egress RSVP: 0 session(s)
```

History

Release version	Command History
3.6.00	This command is enhanced to include a new option that allows the display of RSVP events such as state transitions and events associated with RSVP sessions.
5.1.00	This command is enhanced to display the full LSP name on a single line. Previously, a long LSP name (greater than 12 characters) was text wrapped in multiple lines. Enhanced command: **show mpls rsvp session wide** . The show mpls rsvp session command is enhanced to display if the session is downstream only. Command: **show mpls rsvp session detail**.
5.5.00	This command is enhanced to include the following new filters: • p2mp | p2p - filters RSVP sessions based on type (p2p vs p2mp) • p2mp_id - this is P2MP ID, applicable to P2MP RSVP session types only.
5.8.00	This command is modified to display explicitly on the protected session if it has bandwidth protection or not. It will display only on the protected session. Available on the **show mpls rsvp session detail** command.

show mpls rsvp session backup

Displays the Reserved Reservation Protocol (RSVP) facility backup session.

Syntax

show mpls rsvp session backup [**active** [**brief** | **destination** | **detail** | **egress** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **protection-available** | **protection-unavailable** | **transit** | **up** | **wide**]

Parameters

active
Displays active backup and or detour sessions.

brief
Displays brief session information.

destination
Displays the destination IP address

detail
Displays detailed session information.

egress
Displays the egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessin coming into an interface.

ingress
Displays the ingress session.

name
Displays session by name.

out-interface
Displys RSVP sessions goining out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending state.

protection-available
Displays sessions with protection available.

protection-unavailable
Displays sessions with protection unavailable.

transit

Displays transit session.

up

Displays UP session.

wide

Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the output from the command using the wide option.

```
device#show mpls rsvp session backup wide
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Ingress RSVP: 2 session(s)
To        From            St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.3.3.3  10.2.2.2        Up  SE     -       3        e1/1    tunnel1
10.3.3.3  10.10.10.10(BI) Dn  -      -       -        e1/3    tunnel1
10.3.3.3  10.2.2.2        Up  SE     -       3        e1/1    tunnelfromsanfranciscotonewyork
10.3.3.3  10.10.10.10(BI) Dn  -      -       -        e1/3    tunnelfromsanfranciscotonewyork

Transit RSVP: 0 session(s)
Egress RSVP: 0 session(s)
```

show mpls rsvp session brief

Displays the Reserved Reservation Protocol (RSVP) brief session information.

Syntax

show mpls rsvp session brief [**backup** | **bypass** | **destination** | **detour** | **down** | **egress** | **in-interface** | **ingress name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** | **up**]

Parameters

backup
Displays facility backup session.

bypass
Displays bypass session.

destination
Displays the destination IP address.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

in-interface
Displays RSVP sessions going out on an interface.

ingress
Displays the ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessiond going

p2mp
Displays point to multipoint.

p2p
Displays point to point.

ppend
Displays sessions in soft preemption pending status.

transit
Displays transit session.

up
Displays UP session.

Modes

User EXEC mode

Usage Guidelines

This command operates in all modes.

The **show mpls rsvp session brief** command displays the same information as the **show mpls rsvp session** command.

Command Output

The **show mpls rsvp session brief** command displays the following information:

Output field	Description
Ingress RSVP	Information about ingress RSVP sessions.
Transit RSVP	Information about transit RSVP sessions.
Egress RSVP	Information about egress RSVP sessions.
To	Destination (egress LER) of the session.
From	Source (ingress LER) of the session; the source address for the LSP that was configured with the from command.
St	State can be UP or DOWN.
Style	The RSVP reservation style. Possible values are FF (Fixed Filter), WF (Wildcard Filter), or SE (Shared Explicit).
Lbl_In	The label for inbound packets on this LSP.
Lbl_Out	The label applied to outbound packets on this LSP.
Out_If	The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the *vid* variable.
LSPname	The name of the LSP.

Examples

The following example shows the **show mpls rsvp session** command.

```
device(config)#show mpls rsvp session
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress
Ingress RSVP: 10 session(s)
To           From            St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.22.22.22  10.11.11.11     Up  FF     -       3        e4/3    xmr2
10.33.33.33  10.11.11.11(DI) Up  SE     -       3        e4/4    rj-vpls
10.33.33.33  10.11.11.11     Up  SE     -       1039     e1/15   rj-vpls
..............
Transit RSVP: 1009 session(s)
To           From            St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.22.22.22  10.33.33.33     Up  SE     1024    3        e4/3    2
10.22.22.22  10.33.33.33(DI) Up  SE     1072    1319     e2/4    toxmr2frr-
..............
Egress RSVP: 62 session(s)
To           From            St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.11.11.11  10.22.22.22(DE) Up  SE     3       -        -       toxm1-frr
10.11.11.11 210.22.22.22(DE) Up  SE     3       -        -       toxm1-frr
10.11.11.11 10.22.22.22      Up  SE     3       -        -       toxm1-frr
10.11.11.11 10.44.44.44      Up  FF     3       -        -       toxmr1
```

show mpls rsvp session bypass

Displays *Reserved Reservation Protocol (RSVP)* bypass sessions.

Syntax

show mpls rsvp session bypass [**brief** | **destination** | **detail** | **down** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **up** | **wide**]

Parameters

brief
Displays brief session information.

destination
Destination IP address.

detail
Displays detailed session information.

down
Displays inactive section.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in soft preemption pending status.

up
Displays Up session.

wide
Displays lonf LSP names.

Modes

EXEC mode.

Usage Guidelines

Examples

The following example displays the output of the command with the detail parameter.

```
device# show mpls rsvp session bypass detail
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 2

Ingress RSVP:     2 session(s)
To              From                 St Style Lbl_In  Lbl_Out Out_If LSPname
1.1.4.1         1.1.1.1(BYI)         Up SE    -       1024    ve33
GREEN_DOWN_PE1toP1_VE1111-11.11.1.1-29
  Tunnel ID: 48, LSP ID: 1
  Time left in seconds (PATH refresh: 24, ttd: 4235431
                        RESV refresh: 18, ttd: 113)
  Tspec: peak 19200 kbps rate 19200 kbps size 0 bytes m 20 M 65535
  Setup Priority: 7 Holding Priority: 0
   Session attribute flags:0x04
   (SE Style)
  Explicit path hop count: 3
   11.1.3.0 (S) -> 23.1.100.1 (S) -> 32.1.10.1 (S)
  Received RRO count: 3
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   11.1.3.0 -> 23.1.100.1 -> 32.1.10.1
  PATH sentto:  11.1.3.0        (ve33           ) (MD5 OFF), Message ID: --
  RESV rcvfrom: 11.1.3.0        (ve33           ) (MD5 OFF), Message ID: --
```

show mpls rsvp session destination

Displays the selected Resource Reservation Protocol (RSVP) session destination IP address.

Syntax

show mpls rsvp [**destination** *dest_ip*] [**in-interface** | **out-interface** | **backup** | **brief** | **bypass** | **detail** | **detour** | **egress** | **ingress** | **extensive** | **name** *session_name* | **ppend** | **transit** | **up** | **down** | **wide** | **p2mp** | **p2p**]

Parameters

destination *dest_ip*

Displays the selected destination IP address.

in-interface

Displays RSVP sessions cominf into an interface.

out-interface

Displays RSVP session going out on an interface.

backup

Displays facility backup session.

brief

Display brief session informatiuon.

bypass

Displays bypass session.

detail

Displays detailed session information.

detour

Displays detour session.

egress

Displays egress session.

ingress

Displays ingress session.

extensive

Displays extensive session information.

name *session_name*

Displays session by specified name.

ppend

Displays sessions in soft preemption pending state.

transit

Displays transit session.

up

Displays UP session.

down

Displays inactive session.

wide

Displays long LSP names.

p2mp

Displays point to multipoint sessions.

p2p

Displays point to point sessions.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the output of the command.

```
device(config)#show mpls rsvp session dest 10.30.30.30 source 10.10.10.10 tun 1
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 1
To           From         St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.30.30.30  10.10.10.10  Up  FF     1024    3        e3/1    t1
```

show mpls rsvp session detail

Displays detailed *Reserved Reservation Protocol (RSVP)* session information.

Syntax

show mpls rsvp session detail [**backup** | **bypass** | **destination** | **detour** | **down** | **egress** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** | **up**]

Parameters

backup
Displays facility backup session.

bypass
Displays bypass session.

destination
Destination IP address.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface

p2mp
Displsy point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending state.

transit
Displays transit session.

up
Displays UP session.

Modes

EXEC mode.

Usage Guidelines

Examples

The following example displays the output of the command when the session is only downstream.

```
device# show mpls rsvp session detail
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 1
To              From                St Style Lbl_In  Lbl_Out Out_If LSPname
28.28.28.28     34.34.34.34         Up SE    2050    2049    e1/8   to_NY
  Tunnel ID: 4, LSP ID: 1
  Time left in seconds (PATH refresh: 44, ttd: 119
                        RESV refresh: 7, ttd: 152)
  Tspec: peak 300 kbps rate 300 kbps size 0 bytes m 20 M 65535
  Setup Priority: 7 Holding Priority: 0
   Session attribute flags:0x1f
   (Label recording,SE Style,Protection: Local,Bandwidth,Node)
  Fast Reroute: Facility backup desired
   Setup priority: 7, hold priority: 0
   Bandwidth: 300 kbps, hop limit: 255
   Backup LSP: UP.  Nexthop (node) protection available.
    Bandwidth protection available.
    Up/Down times: 1, num retries: 0
    cost: 0
    Path cspf-group computation-mode: disabled
    Path cspf-computation-mode use-bypass-metric: disabled,
  Explicit path hop count: 2
   93.93.93.9 (S) -> 90.90.90.10 (S)
  Received RRO count: 2
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   93.93.93.9 (P) -> 90.90.90.10
  PATH rcvfrom: 150.150.150.15  (ve11) (MD5 OFF), Message ID: --
  PATH sentto:  93.93.93.9      (e1/8) (MD5 OFF), Message ID: --
  RESV rcvfrom: 93.93.93.9      (e1/8) (MD5 OFF), Message ID: --

To              From                St Style Lbl_In  Lbl_Out Out_If LSPname
28.28.28.28     35.35.35.35(BI)     Up -     2050    3       e1/10  to_NY
  Tunnel ID: 4, LSP ID: 1
  Time left in seconds (PATH refresh: 0, ttd: 4280803)
  Tspec: peak 300 kbps rate 300 kbps size 0 bytes m 20 M 65535
  Setup Priority: 7 Holding Priority: 0
   Session attribute flags:0x06
   (Label recording,SE Style)
  Explicit path hop count: 1
   28.28.28.28 (S)
  PATH rcvfrom: None (downstream only)
  PATH sentto:  28.28.28.28     (e1/10) (MD5 OFF), Message ID: --
  Riding bypass lsp: DUT_16-93.93.93.16-28.28.28.28-2
```

History

Release version	Command history
5.1.00	This command is modified to display when the session is only downstream.

show mpls rsvp session detour

Displays theReserved Reservation Protocol (RSVP) detour session.

Syntax

show mpls rsvp session { **detour** [**active** | **brief** | **detination** | **detail** | **down** | **egress** | **extensive** | **in-interface** | **inactive** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **protection-available** | **protection-unavailable** | **transit** | **up wide**]

Parameters

active
Displaus active backup and detour sessions.

brief
Displays brief session information.

destination
Destination IP address.

detail
Displays detailed sessio information.

down
Displays inactive session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

inactive
Displays inactive, but UP, backup or detour session.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending state.

protection-available
Displays sessions with protection available.

protection-unavailable
Displays sessions with protection unavailable.

transit
Displays transit session.

up
Displays UP session.

wide
Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays a typical output of the command.

```
device# show mpls rsvp session detour
Codes: DI:Ingress Detour  DT:Transir Detour  DM:Merged Detour
       DE:Egress Detour   BI_Ingress Backup  BM:Merged Backup  BE:Egress Backup
       RP:Repaired Session  BYI:Bypass Ingress

Total Number of such sessions are: 0

Ingress RSVP:                0 session(s)

Transit RSVP:             0 session(s)

Egress RSVP:                    0 session(s)
```

show mpls rsvp session down

Displays inactive Reserved Reservation Protocol (RSVP) sessions.

Syntax

show mpls rsvp session down [**backup**| **brief** | **bypass** | **destination** | **detail** | **detour** | **egress** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** | |**wide**]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

bypass
Displays bypass session.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Displays detour session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint session.

p2p
Displays point to point session.

ppend
Displays sessions in a soft preeemption pending state.

transit

Displays transit session.

wide

Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the output of the command using the wide option.

```
device#show mpls rsvp session down wide
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress
Total Number of such sessions are: 59
Transit RSVP:   59 session(s)
To              From                St Style Lbl_In  Lbl_Out Out_If LSPname
10.0.11.11      10.0.0.5            Dn -     -       -       e1/2   to_AR11_autoBW_11
10.0.11.12      10.0.0.5            Dn -     -       -       e1/2   to_AR11_autoBW_12
10.0.11.13      10.0.0.5            Dn -     -       -       e1/2   to_AR11_autoBW_13
10.0.11.14      10.0.0.5            Dn -     -       -       e1/2   to_AR11_autoBW_14
```

show mpls rsvp session extensive

Displays extensive Reserved Reservation Protocol (RSVP) session information.

Syntax

show mpls rsvp session extensive [**backup** | **bypass** | **destination** | **detour** | **down** | **egress** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** | **up**]

Parameters

backup
Displays facility backup session.

bypass
Displays bypass session.

destination
Destination IP address.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress sessions.

name
Displays sessionn by name.

out-interface
Displays RSVP sessions going out of an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending state.

transit
Displays transit session.

up
Displays UP sessions.

Modes

User EXEC mode

Usage Guidelines

Command Output

The **show mpls rsvp session extensive** command displays the following information:

Output field	Description
Ingress RSVP	Displays information about ingress RSVP sessions.
Transit RSVP	Displays information about transit RSVP sessions.
Egress RSVP	Displays information about egress RSVP sessions.
From	Source (ingress LER) of the session; the source address for the LSP that was configured with the **from** command.
St	State can be UP or DOWN.
Style	The RSVP reservation style. Possible values are Fixed Filter (FF), Wildcard Filter (WF), or Shared Explicit (SE).
Lbl_In	The label for inbound packets on this LSP.
Lbl_Out	The label applied to outbound packets on this LSP.
Out_If	The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the *vid* variable.
LSPname	The name of the LSP.
Time left in seconds	The amount of time left for the PATH or RESV refreshes.
Tspec	Traffic engineering specification for the LSP, including the max-rate ("peak"), mean rate ("rate"), number of burst bytes ("size"), maximum policed unit ("M"-or maximum packet size), and minimum policed unit ("m"-or minimum packet size).
Explicit path hop count	The number of explicit hops used in this RSVP session.
Received RRO count	The number of Record Route Objects received on this RSVP session.
PATH sentto	Address of the next LSR in the LSP, and the interface used to reach this LSR. When applicable, 'PATH sentto' displays a VE interface specified by the *vid* variable.
PATH rcvfrom	Address of the previous LSR in the LSP, and the interface used to reach this LSR. When the session is downstream only, then it is displayed. When applicable, 'PATH rcvfrom' displays a VE interface specified by the *vid* variable.
PATH history	Displays history of the last 20 RSVP event. Each event contains: • Event index (used to provide the number of events). • Time stamp • File name and line number where the event is logged. • Event description and extra information associated with each event.

Examples

The following example displays the command output containing the contents of the History buffer for the last 20 RSVP events.

```
device# show mpls rsvp session extensive
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Ingress RSVP: 7 session(s)
To          From            St Style Lbl_In Lbl_Out Out_If LSPname
10.33.33.33 10.11.11.11(DI) Up SE    -      3       e4/4   rj-vpls
 Tunnel ID: 1, LSP ID: 1
 Time left in seconds (PATH refresh: 10, ttd: 4288020
                       RESV refresh: 0, ttd: 4288177)
 Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
 Explicit path hop count: 1
  10.0.0.6 (S)
 Received RRO count: 1
  Protection codes/Rtr Id flag: P: Local N: Node B: Bandwidth I: InUse R: RtrId
  10.0.0.6
 Detour Sent: Number of PLR and Avoid Node ID pair(s): 1
  [1]: PLR: 10.1.1.1 Avoid Node: 10.1.1.2
 PATH sentto: 10.0.0.6 (e4/4) (MD5 OFF)
 RESV rcvfrom: 10.0.0.6 (e4/4) (MD5 OFF)
 PATH history:
  1 Dec 10 11:57:59 Query route to 10.33.33.33: nhop 10.0.0.6
  2 Dec 10 11:57:59 Tx PATH: out if(e4/4), flg(0x01000500/0x0000000a)
  3 Dec 10 11:57:59 Rx RESV: label(3), flg(0x01000500/0x0000000a)
  4 Dec 10 11:57:59 Tx cnnt req: hdl(0x0010c001), flg(0x01100500/0x0000000a)
  5 Dec 10 11:57:59 Start TC event(NEW_FLOW): action(0x0000000a)
  6 Dec 10 11:57:59 Rx cnnt resp: hdl(0x0010c001), flg(0x01100500/0x0000000a)
  7 Dec 10 11:57:59 Complete TC event(NEW_FLOW)
 RESV history:
  1 Dec 10 11:57:59 Add RSB: style(SE), filterSpec(1), flg(0x00000000)
  2 Dec 10 11:57:59 Add filterSpec: 10.11.11.11/1, label(3)
```

History

Release version	Command history
3.6.00	This command was enhanced to include a new option that allows the display of RSVP events such as state transitions and events associated with RSVP sessions.

show mpls rsvp session (ingress/egress)

Displays Reserved Reservation Protocol (RSVP) ingress or egress session.

Syntax

show mpls rsvp session ingress [**backup** | **brief** | **bypass** | **destination** | **detail** | **detour** | **down** | **extensive** | **in-interface** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **up** | **wide**]

show mpls rsvp session egress [**backup** | **brief** | **destination** | **detail** | **detour** | **down** | **extensive** | **in-interface** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **up** | **wide**]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

bypass
(For **ingress** only) Displays bypass session information.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Dsiplays detour session.

down
Displays inactive session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending status.

up

Displays UP session.

wide

Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

show mpls rsvp session (interface)

Displays RSVP sessions that are coming into (in-interface) or going out to (out-interface) an interface.

Syntax

show mpls rsvp session in-interface { **ethernet** *slot* **/** *port* | **pos** *slot* **/** *port* | **ve** *interface_id* }

show mpls rsvp session out-interface { **ethernet** *slot* **/** *port* | **pos** *slot* **/** *port* | **ve** *interface_id* }

Parameters

ethernet *slot* **/** *port*

Displays the specified Ethernet port.

pos *slot* **/** *port*

Displays the specified POS port.

ve *interface_id*

Displays the specified Virtual Ethernet Interface ID.

Modes

User EXEC mode

Usage Guidelines

show mpls rsvp session name

Displays the Reserved Reservation Protocol (RSVP) session by name.

Syntax

show mpls rsvp session name *session_name* [[**backup** | **brief** | **bypass** | **destination** | **detail** | **detour** | **down** | **egress** | **extensive** | **in-interface** | **ingress** | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** | **up** | **wide**] **extensive**]

Parameters

backup
Displays facility backup session information.

brief
Displays brief session information.

bypass
Display bypass session information.

destination
Destination IP address information.

detail
Displays detailed session information.

detour
Displays detour session information.

down
Displays inactive session information.

egress
Displays egress session information.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session information.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint session information.

p2p
Displays point to point session information.

ppend
Displays sessions in the soft preemption pending state.

transit

Displays transit session information.

up

Displays up session information.

wide

Displays the long LSP name.

Modes

User EXEC mode

Usage Guidelines

Command Output

The **show mpls rsvp session name** command displays the following information:

Output field	Description
To	Destination (egress LER) of the session.
From	Source (ingress LER) of the session; the source address for the LSP that was configured with the **from** command.
St	State can be UP or DOWN.
Style	The RSVP reservation style. Possible values are FF (Fixed Filter), WF (Wildcard Filter), or SE (Shared Explicit).
Lbl_in	The label for inbound packets on this LSP.
Lbl_out	The label applied to outbound packets on this LSP.
Out_if	The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the *vid* variable.
LSPname	The name of the LSP.
Tunnel ID	A numerical value that identifies the tunnel being configured.
Time left in seconds	The amount of time left for the PATH or RESV refreshes.
Tspec	Traffic engineering specification for the LSP, including the max-rate (“peak”), mean rate (“rate”), number of burst bytes (“size”), maximum policed unit (“M”—or maximum packet size), and minimum policed unit (“m”—or minimum packet size).
Setup Priority	An LSPs setup priority is considered during admission control, and its hold priority is considered when bandwidth is allocated to the LSP. The setup priorities are expressed as numbers between zero (0) (highest priority level) and seven (7) (lowest priority level).
Holding Priority	The hold priority is considered when bandwidth is allocated to the LSP. The hold priorities are expressed as numbers between zero (0) (highest priority level) and seven (7) (lowest priority level).
Received RRO count	The number of Record Route Objects received on this RSVP session.
PATH sentto	Address of the next LSR in the LSP, and the interface used to reach this LSR. When applicable, PATH sentto displays a VE interface specified by the *vid* variable.
PATH history	Displays history of the last 20 RSVP events. Each event contains: • Event index (used to provide the number of events). • Time stamp.

Output field	Description
	• File name and line number where the event is logged. • Event description and extra information associated with each event.
RESV history	Displays reservation history.
Session history	Displays session history.
Packet Type	
Path	The number of Path messages sent and received. Path messages store information about the state of the path along the LSRs in the LSP.
Resv	The number of RESV messages sent and received. RESV messages include FF (Fixed Filter), WF (Wildcard Filter), and SE (Shared Explicit) messages.
PathErr	The number of PathErr messages sent and received.
RevErr	The number of ResvErr messages sent and received.
PathTear	The number of PathTear messages sent and received. PathTear messages cause path states to be deleted.
ResvTear	The number of ResvTear messages sent and received. ResvTear messages cause reservation states to be deleted.
ResvConf	The number of reservation confirmation messages sent and received.
Error	
PATH state timeout	The PATH timeout.
RESV state timeout	The reservation confirmation timeout.
Rcv pkt proc error	
Path	The number of Path messages received with a packet processing error.
Resv	The number of RESV messages received with a packet processing error.
PathErr	The number of PathErr messages received with a packet processing error.
RevErr	The number of ResvErr messages received with a packet processing error.
PathTear	The number of PathTear messages received with a packet processing error.
ResvTear	The number of reservation confirmation messages received with a packet processing error.
ResvConf	The number of reservation confirmation messages received with a packet processing error.

Examples

The following example shows how the protocol statistics display when using the **extensive** option.

```
device# show mpls rsvp session name lsp1 extensive
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 1
To              From                St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
14.14.14.14     12.12.12.12         Up  FF     -       3        e2/1    lsp1
  Tunnel ID: 1, LSP ID: 1
  Time left in seconds (PATH refresh: 26, ttd: 3889074
                        RESV refresh: 4,  ttd: 141)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
  Setup Priority: 7 Holding Priority: 0
   Session attribute flags:0x00
  Received RRO count: 1
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   22.22.22.14
  PATH sentto:  22.22.22.14     (e2/1           ) (MD5 OFF), Message ID: 1
  RESV rcvfrom: 22.22.22.14     (e2/1           ) (MD5 OFF), Message ID: --
  PATH history:
    1 Dec 11 20:40:23 Add PSB: tunnel endpt 14.14.14.14/12.12.12.12
<SNIP>
   17 Dec 11 20:40:23 Tx Resv to TE-MIB: flg(0x00005404/0x00000000)
  RESV history:
    1 Dec 11 20:40:23 Add RSB: style(FF), filterSpec(1), flg(0x00000000)
    2 Dec 11 20:40:23 Add filterSpec: 12.12.12.12/1, label(3)

  Session history:
    1 Dec 11 20:40:23 A new PSB 0x30ee03c8 created. stack[1]=0x00000001 stack[2]=0x21bab8d4
<SNIP>
   12 Dec 11 20:40:23 TC-action LDB_CONNECT completed

                         Protocol Stats
                       Since Last Clear
Packet Type              Sent  Received
Path                        1         0
Resv                        0                   1
PathErr                     0         0
RevErr                      0         0
PathTear                    0         0
ResvTear                    0         0
ResvConf                    0         0


Error                  Since Last Clear
PATH state timeout                  0
RESV state timeout                  0


Rcv pkt proc error:    Since Last Clear
Path                        0         0
Resv                        0         0
PathErr                     0         0
RevErr                      0         0
PathTear                    0         0
ResvTear                    0         0
ResvConf                    0         0
```

History

Release version	Command history
5.9.00	This command was modified to show the protocol statistics under the **extensive** option.

show mpls rsvp session p2mp

Displays Reserved Reservation Protocol (RSVP) point-to-multipoint sessions.

Syntax

show mpls rsvp session p2mp [**brief** | **detail** | **down** | **egress** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp-id** | **ppend** | **s21** | **transit** | **up** | **wide**]

Parameters

brief

Displays brief session information.

detail

Displays detailed session information.

down

Displays inactive session.

egress

Displays egress sesson.

extensive

Displays extensive session information.

in-interface

Displays RSVP sessions coming into an interface.

ingress

Displays ingress session.

name

Displays session by name. Some vendors allow each S2L sub-LSP for a P2MP LSP to have a different name. With such configurations in place the name filter responds in two different ways based on what other filters are applied in conjunction to the name filter.

- When the name filter is applied with p2mp filter and without and s2l filter, the entire P2MP session displays with all the S2L sub-LSPs in the detail format by default even if one of the S2L sub-LSP name matches with the supplied name in the CLI.
- When the name filter is applied with both p2mp filter and s2l filter, only that S2L-sub LSP whose name matches the name supplied displays along with the P2MP session's common information in detail format.
- When name filter is applied with out-interface filter, only that S2L which matches both criteria displays.
- By default, in the common part of the P2MP session information, the name displayed would be the name of the first S2L-sub LSP displays in the detail format when no s2l filter is applied.

out-interface

Displays RSVP sessions going out on an interface. The out-interface filter would filter and display only those p2mp S2Ls that are going out via the interface requested. Other S2Ls not going out of the interface requested would not be displayed. The part common to all the S2Ls for a P2MP LSP displays first in the detail format followed by the S2L information.

p2mp-id

P2MP ID. It is the IP address picked from PE1 (Ingress), which could be same for multiple P2MP sessions originating from PE1. The P2MP ID is not a loopback address and may be any 32 bit number. The P2MP ID can also be local IP address. The P2MP-ID can be in Ip address or decimal format.

ppend

Displays sessions in soft preemption pending state.

s21

Displays point to multipoint source to leaf sub-LSPs.

transit

Displays transit session.

up

Displays UP session.

wide

Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the output of the command.

```
device# show mpls rsvp session p2mp
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress
Total Number of such sessions are: 2

Ingress RSVP:     0 session(s)
Transit RSVP:     2 session(s)

P2MP_Id           From         Tunnel_Id  Style  Lbl_In  Num_S2l  LSPname
10.10.10.1        7.7.7.6      45         SE     1037    3        to-pe2
10.10.10.1        5.5.5.1      43         FF     3021    1        to-nyc

Egress RSVP:      0 session(s)
```

The following example displays the command with the wide option.

```
device# show mpls rsvp session p2mp s2l wide
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress
Total Number of such sessions are: 2

Ingress RSVP:     0 session(s)
Transit RSVP:     2 session(s)

P2MP_ID          From           Tunnel_ID  Style  Lbl_In  Num_S2L  LSPname
10.10.10.1       7.7.7.6        45         SE     1037    3        to-pe2

To               From           St Style  Lbl_In  Lbl_Out Out_If   LSPname
92.92.94.48      7.7.7.6        Up SE     1037    1028    ve101    to-pe2
92.92.95.48      7.7.7.6        Up SE     1037    1028    ve101    to-pe3
92.92.96.48      7.7.7.6        Up SE     1037    1028    ve101    to-pe4
```

The following example displays the command using the option P2MP-ID. The P2MP-ID can be in Ip address or decimal format.

```
device# show mpls rsvp session p2mp p2mp-id 168430081

Total Number of such sessions are: 1
Ingress RSVP:     0 session(s)
Transit RSVP:     1 session(s)

P2MP_ID         From           Tunnel_ID  Style  Lbl_In  Num_S2L   LSPname
168430081       7.7.7.6        45         SE     1037    3         to-pe2

Egress RSVP:     0 session(s)

device#show mpls rsvp sess p2mp p2mp-id 20.0.0.1

Total Number of such sessions are: 1
Ingress RSVP:     0 session(s)
Transit RSVP:     1 session(s)

P2MP_ID         From           Tunnel_ID  Style  Lbl_In  Num_S2L   LSPname
10.10.10.1      7.7.7.6        45         SE     1037    3         to-pe2

Egress RSVP:     0 session(s)
```

The following example displays the output of the command with the detail option. The first part of the command displays the attributes and information that are common to all S2ls of the P2MP LSP. The second part displays information about each of the individual S2L sub LSP. In this output, there are two S2Ls for the session.

```
device# show mpls rsvp session p2mp detail

Total Number of such sessions are: 1

Ingress RSVP:     0 session(s)
P2MP_Id              From               Tunnel_Id  Style  Lbl_In  Num_S2L   LSPname
10.10.10.1           7.7.7.6            45         SE     1037    3         to-pe2

  Tspec: peak 1 kbps rate 1 kbps size 0 bytes m 20 M 65535
  Setup Priority: 7 Holding Priority: 0
   Session attribute flags:0x04(SE Style)

To                   From                St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
92.92.94.48          7.7.7.6             Up  SE     1037    1028     ve101   to-pe2

  LSP ID: 2, Sub-group Originator ID: 7.7.7.6 Sub-group ID: 2
  Time left in seconds (PATH refresh: 0, ttd: 133
                        RESV refresh: 0, ttd: 136)
  Explicit path hop count: 2
   7.1.13.2 (S) -> 21.21.21.1 (S) -> 31.31.31.1(S)
  Received RRO count: 2

   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   7.1.13.2 -> 21.21.21.1 -> 31.31.31.1

  PATH rcvfrom: 7.1.18.2        (e4/1)            (MD5 OFF), Message ID: 75
  PATH sentto:  7.1.13.2        (ve101)           (MD5 OFF), Message ID: 2575
  RESV rcvfrom: 7.1.13.2        (ve101)           (MD5 OFF), Message ID: 54024

To                  From                St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
92.92.95.48         7.7.7.6             Up  SE     1037    1028     ve101   to-pe3

  LSP ID: 2, Sub-group Originator ID: 7.1.18.2 Sub-group ID: 2
  Time left in seconds (PATH refresh: 0, ttd: 143
                        RESV refresh: 0, ttd: 121)
  Explicit path hop count: 3
   7.1.13.2 (S) -> 21.21.21.1 (S)-> 41.41.41.1 (S)
  Received RRO count: 3
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   7.1.13.2 -> 21.21.21.1 -> 41.41.41.1
  PATH rcvfrom: 7.1.18.2        (e4/1)            (MD5 OFF), Message ID: 77
  PATH sentto:  7.1.13.2        (ve101)           (MD5 OFF), Message ID: 2577
  RESV rcvfrom: 7.1.13.2        (ve101)           (MD5 OFF), Message ID: 54026
<SNIPPED output for 3rd S2L>
Egress RSVP:     0 session(s)
```

History

Release version	Command history
5.5.00	This command was modified to include the P2MP option.

show mpls rsvp session p2p

Displays Reserved Reservation Protocol (RSVP) point-to-point sessions.

Syntax

show mpls rsvp session p2p [**backup** | **brief** | **bypass** | **destination** | **detail** | **detour** | **down** | **egress** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **ppend** | **transit** | **up** | **wide**]

Parameters

backup
Displays facility backup session information.

brief
Displays brief session information.

bypass
Displays bypass session.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Dosplays RSVP sessions coming into an interface.

ingress
Dsiplays ingress session.

name
Disolays session by name.

out-interface
Displays RSVP sessions going out on an interface.

ppend
Displays sessions in a soft preeemption pending state.

transit
Dsiplays transit session.

up

Displays UP session.

wide

Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

History

Release version	Command history
5.5.00	This command was modified to include the P2P option.

show mpls rsvp session ppend

Displays Reserved Reservation Protocol (RSVP) sessions that are in a soft preemption state.

Syntax

show mpls rsvp session ppend [**brief** | **destination** | **detail** | **down** | **egress** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **transit** | **up** | **wide**]

Parameters

brief
Displays brief session information.

destination
Destination IP address.

detail
Displays detailed session information.

down
Displays inactive session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint session.

p2p
Displays point to point session.

transit
Displays transit session.

up
Displays Up session.

wide
Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the appended view of the session.

```
device(config-mpls-lsp-high)#show mpls rsvp sess ppend
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 1

Transit RSVP: 1 session(s)
To           From         St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
80.80.80.80  40.40.40.40  Up  SE     1024    3        e1/7    1
```

show mpls rsvp session transit

Displays Reserved Reservation Protocol (RSVP) transit sessions.

Syntax

show mpls rsvp session transit [**backup** | **brief** | **destination** | **detail** | **detour** | **down** | **extensive** | **in-interface** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **statistics** | **up** | **wide**]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Displays detour session.

down
Displays inactive session.

extensive
Displays extensive session information.

in-interface
Displays RSVP session coming into an interface.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions on a soft preemption pending state.

statistics
Displays transit LSP traffic statistics.

up
Displays UP session.

wide

Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays when at least one LP does not support all three statistics.

```
device# show mpls rsvp session transit statistics
* means statistics collection is not supported on one or more of the line cards

Total Number of such sessions are: 4

To              From            Packets   Bytes     Rate(kbps)   LSPname
150.150.150.10  190.190.190.9   1007      7654903*  53556*          test1
150.150.150.10  190.190.190.9   0         0*           0*              test2
```

The following example displays when all of the LPs support all three statistics.

```
device# show mpls rsvp session transit statistics
* means statistics collection is not supported on one or more of the line cards

Total Number of such sessions are: 4

To              From            Packets   Bytes      Rate(kbps)   LSPname
150.150.150.10  190.190.190.9   1007      7654903    53556           test1
150.150.150.10  190.190.190.16  626241    56255         485             test2
150.150.150.10  190.190.190.9   65946     35648469   63582           test3
150.150.150.10  190.190.190.9   0         0             0               test4
```

History

Release version	Command history
5.4.00	This command was modified to include the keyword "statistics".

show mpls rsvp session up

Displays the number of UP Reserved Reservation Protocol (RSVP) sessions.

Syntax

show mpls rsvp session up [**backup** | **brief** | **bypass** | **destination** | **detail** | **detour** | **egress** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** |**wide**]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

bypass
Displays bypass session.

destination
Destination IP address.

detail
Displays detailes session information.

detour
Displays detour session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending status.

transit

Displays transit session.

wide

Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the command using the wide option.

```
device#show mpls rsvp session up wide
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 59946
Transit RSVP: 59439 session(s)

To              From                St Style Lbl_In  Lbl_Out Out_If LSPname
172.16.20.1     172.16.50.1         Up SE    58368   3       e15/2  LSP-63301
172.16.22.1     172.16.30.1         Up SE    15873   23328   e21/6  LSP-10002
172.16.22.1     172.16.32.1(BI)     Up -     15873   45255   e1/2   LSP-10002
172.16.22.1     172.16.30.1         Up SE    54733   49673   e15/1  LSP-10003
172.16.22.1     172.16.32.1(BI)     Up -     54733   43841   e1/2   LSP-10003
172.16.22.1     172.16.30.1         Up SE    19472   15317   e1/8   LSP-10006
172.16.22.1     172.16.32.1(BI)     Up -     19472   15317   e1/2   LSP-10006
```

show mpls rsvp session wide

Displays Reserved Reservation Protocol (RSVP) sessions with long LSP names.

Syntax

show mpls rsvp session wide [**backup**| **bypass** | **destination** | **detour** | **down** | **egress** | **in-interface**| **ingress** | **name** | **out-interface** | **p2mp** | **p2p** | **ppend** | **transit** | **up**]

Parameters

backup
Displays facility backup session.

bypass
Displays bypass session.

destination
Destination IP address.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending status.

transit
Displays transit session.

up
Displays UP session.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the output of the command.

```
device#show mpls rsvp session wide
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 1611

Ingress RSVP:  1088 session(s)
To              From                St Style Lbl_In  Lbl_Out Out_If LSPname
3.3.3.1         2.2.2.1             Up SE    -       3       ve207  to-nakul-156-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve205  to-nakul-179-3.3.3.1
3.3.3.1         2.2.2.1             Up FF    -       3       ve225  to-nakul-4
3.3.3.1         2.2.2.1             Up SE    -       3       ve218  to-nakul-17-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve209  to-nakul-8-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve206  to-nakul-55-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve216  to-nakul-40-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve220  to-nakul-194-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve204  to-nakul-78-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve213  to-nakul-212-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve217  to-nakul-141-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve208  to-nakul-32-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve215  to-nakul-164-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve223  to-nakul-197-3.3.3.1
3.3.3.1         2.2.2.1             Up SE    -       3       ve225  to-nakul-174-3.3.3.1

device#
```

History

Release version	Command history
5.1.00	This command was modified to include the wide option. This option displays the full LSP name on a single line.

show mpls rsvp statistics

Displays the RSVP control packet statistics combined over all the interfaces.

Syntax

show mpls rsvp statistics

Modes

User EXEC mode

Usage Guidelines

The device constantly gathers RSVP statistics. RSVP statistics are collected from the time RSVP is enabled, as well as from the last time the RSVP statistics counters were cleared.

The command resets the counters listed under the 'Since last clear' column for the **show mpls rsvp interface detail** and **show mpls rsvp statistics** commands.

This command operates in all modes.

Command Output

The **show mpls rsvp statistics** command displays the following information:

Output field	Description
Path	The number of Path messages sent and received. Path messages store information about the state of the path along the LSRs in the LSP.
Resv	The number of RESV messages sent and received. RESV messages include Fixed Filter (FF), Wildcard Filter (WF), and Shared Explicit (SE) messages.
PathErr	The number of PathErr messages sent and received.
ResvErr	The number of ResvErr messages sent and received.
PathTear	The number of PathTear messages sent and received. PathTear messages cause path states to be deleted.
ResvTear	The number of ResvTear messages sent and received. ResvTear messages cause reservation states to be deleted.
ResvConf	The number of reservation confirmation messages sent and received.
Rcv pkt bad length	The number of times a packet was not processed because it was the wrong length.
Rcv pkt unknown type	The number of times an RSVP packet was not processed because it was not one of the types defined in RFC 2205.
Rcv pkt bad version	The number of times a packet was not processed because it was an RSVP version other than one.
Rcv pkt bad cksum	The number of times a packet was not processed because of a bad RSVP checksum.
Memory alloc fail	The number of times a packet was not processed because RSVP memory allocation failed on the device.

TABLE 14 Rcv pkt processing errors

Output field	Description
Path	The number of Path messages received with a packet processing error.
Resv	The number of RESV messages received with a packet processing error.
PathErr	The number of PathErr messages received with a packet processing error.
ResvErr	The number of ResvErr messages received with a packet processing error.
PathTear	The number of PathTear messages received with a packet processing error.
ResvTear	The number of reservation confirmation messages received with a packet processing error.
ResvConf	The number of reservation confirmation messages received with a packet processing error.

Examples

The following example displays the **show mpls rsvp statistics** command output.

```
device# show mpls rsvp statistics
Total Since last clear
PacketType Sent Received Sent Received
Path 4 4 4 4
Resv 4 4 4 4
PathErr 0 0 0 0
ResvErr 0 0 0 0
PathTear 0 0 0 0
ResvTear 0 0 0 0
ResvConf 0 0 0 0
Errors Total Since last clear
Rcv pkt bad length 0 0
Rcv pkt unknown type 0 0
Rcv pkt bad version 0 0
Rcv pkt bad cksum 0 0
Memory alloc fail 0 0
Rcv pkt processing error:
Path 0 0
Resv 0 0
PathErr 0 0
ResvErr 0 0
PathTear 0 0
ResvTear 0 0
ResvConf 0 0
```

History

Release version	Command history
5.6.00	The 'Hello' packet type was added. The **clear mpls rsvp statistics** command clears the 'since last clear' column for the 'Hello' packet type.

show mpls static-lsp

Displays the static LSPs in the system.

Syntax

show mpls static-lsp [**brief** | **debug** | **detail**| **wide**]

show mpls static-lsp extensive [**descending**]

show mpls static-lsp name *lsp-name* **extensive** [**descending**]

show mpls static-lsp { **down** | **up** } [**detail** | **wide** | **extensive** [**descending**]]

Parameters

brief
Displays brief information.

debug
Displays debug information, with history.

detail
Displays detailed information.

wide
Displays long LSP names.

extensive
Displays detailed information with History.

descending
Displays LSP History with newer entries on top.

name *lsp-name*
Displays information by LSP name.

down
Displays operationally DOWN LSPs.

detail
Displays detailed information of the operationally DOWN LSPs.

extensive
Displays detailed information with History of the operationally DOWN LSPs.

wide
Displays long LSP names of the operationally DOWN LSPs.

up
Displays operationally UP LSPs.

Modes

User EXEC mode

Command Output

The **show mpls static-lsp** command displays the following information:

Output field	Description
Name	Name of the static LSP as configured by the user.
Admin	Whether or not the static LSP is enabled.
Oper	Operational state of the LSP.
In-label	The in-label configured for the LSP.
Out-label	The out-label configured. If none, the implicit-null label 3 is shown.
Next-hop	The configured next-hop.
Out-Intf	The out-interface that corresponds to the next-hop configured.

The **show mpls static-lsp extensive** command displays the following information:

Output field	Description
Role	The role of the LSP. Only transit.
Enabled	Whether the LSP is enabled or not.
Times LSP goes UP since enabled	Number of times the LSP has gone UP since being enabled.
In-label	The in-label configured for the LSP.
Next-hop	The configured next-hop.
History	The static-lsp sample History.
Static-LSP	Identifier of the static-LSP.
Role	The role of the LSP. Currently, only transit.
Enabled	Whether the LSP is enabled or not.
UP	Whether LSP is operational or not.
LSP error	Reason LSP is down or if there was any error during any processing on the LSP.
Times LSP goes UP since enabled	Number of times the LSP has gone UP since being enabled.
In-label	The in-label configured for the LSP.
Out-label	The configured out-label, three if implicit-null.
Next-hop	The configured next-hop.
Out-interface for the next-hop	The out-interface that corresponds to the configured next-hop.
Next-hop interface address to reach configured next-hop	The interface address to reach the next-hop address configured. It is the same as the configured next-hop in case the configured next-hop address is directly connected and different if not directly-connected.

Examples

The following example displays the output of the **show mpls static-lsp** command.

```
device# show mpls static-lsp
Number of transit lsps: 2
Name    Admin   Oper  In-label Out-label  Next-hop         Out-Intf
c2      UP      DOWN  21       1024       160.168.123.122  e2/1
c3      UP      UP    22       3          160.168.111.100  ve10
```

The following example displays the output of the **show mpls static-lsp extensive** command.

```
device# show mpls static-lsp extensive
Static-LSP t1, Role: Transit
  Enabled: Yes, UP: Yes
  Times LSP goes up since enabled: 1
  In-label: 201, Out-label: 3,
  Next-hop: 120.120.120.2,
  Out-Interface for the next-hop: e2/1
  Next-hop interface address to reach configured next-hop: 10.1.1.2
  History
    0 Jul 11 01:38:32 : LSP tunnel is Enabled
    1 Jul 11 01:38:33 : Static Transit LSP UP
Static-LSP t2, Role: Transit
  Enabled: Yes, UP: No
  LSP error: No interface available for next-hop
  Times LSP goes up since enabled: 1
  In-label: 202, Out-label: 3,
  Next-hop: 20.1.1.2,
  Out-Interface for the next-hop: --
  Next-hop interface address to reach configured next-hop: --
  History
    0 Jul 11 01:38:32 : LSP tunnel is Enabled
```

History

Release version	Command history
5.8.00	This command was modified to include the keyword "descending" to display the LSP History in reverse chronological order.

show mpls statistics 6pe

Displays IPv6 over MPLS statistics.

Syntax

show mpls statistics 6pe [*slot/port* | **vrf**]

Parameters

slot/port

Displays MPLS statistics for the specified interface number.

vrf

Displays statistics based on VRFs.

Modes

User EXEC mode

Usage Guidelines

This command operates in all modes.

The **clear mpls statistics 6pe** *slot/port* command clears the 6pe statistics.

Examples

The following example displays the number of 6PE packets going into or coming out of the MPLS cloud. The packet counter is per PPCR.

```
device# show mpls statistics 6pe
In-Port(s)       Endpt Out-Pkt            Tnl Out-Pkt
e2/1 - e2/4      0                   0
e2/5 - e2/8      0                   0
e4/1 - e4/2      41810353            0
e4/3 - e4/4      0                   41810352
device
```

The following example displays the number of IPv6 packets from a provider edge (PE) router going into or coming out of the MPLS cloud.

```
device> show mpls statistics 6pe

In-Port(s)      Endpt Out-Pkt      Tnl Out-Pkt
e1/1 - e1/2     184116072          1697803327
e1/3 - e1/4     389547885          6036111
e2/1 - e2/24    1088610            0
e2/25 - e2/48   0                  248406
e3/1            2045067126         5288598554
e3/2            0                  0
```

show mpls statistics bypass-lsp

Displays the incoming packet count and byte count rate (in bytes) on a tunnel interface for bypass LSPs.

Syntax

show mpls statistics bypass-lsp *lsp-name*

Parameters

lsp-name

The name of the specified LSP.

Modes

User EXEC mode

Examples

The following example shows the **show mpls statistics bypass-lsp** *lsp-name* command.

```
device# show mpls statistics bypass-lsp
LSP B1
  Tunnel interface   tnl4  100 pkt  2200 Byte Last Update Dec 17 18:51:21.000
LSP B1
  Tunnel interface   tnl6  900 pkt  33445 Byte Last Update Dec 17 18:51:38.000
LSP B1
  Tunnel interface   tnl9  78 pkt  7229 Byte Last Update Dec 17 18:51:41.000
LSP B1
  Tunnel interface   tnl15  456 pkt  2398 Byte Last Update Dec 17 18:52:1.000
```

History

Release version	Command history
5.7.00	This command was introduced.

show mpls statistics label

Displays statistics for LDP ECMP paths.

Syntax

show mpls statistics label

Parameters

label

Displays the in-label statistics.

Modes

User EXEC mode

Usage Guidelines

Command Output

The **show mpls statistics label** command displays the following information:

Output field	Description
In-label	The MPLS label ID.
In-Port (s)	The port where the traffic arrives.
In-Packet Count	The number of packets meeting the In-label and In-port criteria.
In-Bytes Count	The number of bytes meeting the In-label and In-port criteria.

Examples

The following example displays all of the MPLS traffic statistics by their MPLS label.

```
device# show mpls statistics label
In-label   In-Port(s)      In-Packet Count
1024       e3/1            315431
           e3/2            349193
           e3/3            0
           e3/4            0
1025       e3/1            419750
           e3/2            0
           e3/3            0
           e3/4            0
1024       e5/1 - e5/10    364690
           e5/11 - e5/20   0
           e5/21 - e5/30   0
1025       e5/1 - e5/10    0
           e5/11 - e5/20   0
           e5/21 - e5/30   0
```

The following example displays all the MPLS traffic statistics by their MPLS label for a Brocade NetIron CES Series or Brocade NetIron CER Series device.

```
device# show mpls statistics label
In-label  In-Port(s)    In-Bytes Count
1024      e1/1-e1/24    315431
          e1/25-e1/48   0
```

The following example displays all MPLS traffic statistics, by their MPLS label, which are gathered by the corresponding network processor.

```
device# show mpls statistics label 3/1
In-label     In-Port(s)      In-Packet Count
1024         e3/1 - e3/20    30
1026         e3/1 - e3/20    21
1030         e3/1 - e3/20    100
1032         e3/1 - e3/20    0
1033         e3/1 - e3/20    0
1034         e3/1 - e3/20    12
1036         e3/1 - e3/20    0
```

The following example displays all MPLS traffic statistics by their MPLS label for a specific port on a Brocade NetIron CES Series or Brocade NetIron CER Series device.

```
device# show mpls statistics label 1/1
In-label    In-Port(s)      In-Bytes count
1024        el/1-el/24      315431
```

History

Release version	Command history
5.1.00	This command was modified to display statistics for LDP ECMP paths.

show mpls statistics ldp transit

Displays the traffic statistics for transit LDP FECs.

Syntax

show mpls statistics ldp transit [**fec** *ip-addr* [**/***subnet-mask*]]

Parameters

fec *ip_addr*

Displays the traffic statistics for the transit LDP FECs.

IP-subnet-mask

Specifies an IP subnet-mask length.

Modes

User EXEC mode

Usage Guidelines

This command operates in all modes.

Packet count is not available for Brocade NetIron CES Series and Brocade NetIron CER Series devices.

Command Output

The **show mpls statistics ldp transit** command displays the following information:

Output field	Description
FEC	The specified FEC for MPLS LDP transit statistics.
Packets	Specifies the number of packets received.
Bytes	Specifies the number of bytes received.
Rate-kbps	Rate is in kilobits per second.

Examples

The following example displays output from the **show mpls statistics ldp transit** command:

```
device# show mpls statistics ldp transit
FEC               Packets    Bytes       Rate-kbps
10.35.3.0/30      0          0*          0*
10.35.10.1/32     0          0*          0*
10.255.245.214/32 112        7566182*    6224*
192.168.37.36/30  532114     2350644*    564*
```

* means statistics collection is not supported on one or more of the line cards.

The following example displays output from the **show mpls statistics transit** command with the **fec** keyword:

```
device# show mpls statistics ldp transit fec 10.255.245.214
FEC                Packets    Bytes       Rate-kbps
10.255.245.214/32  112        7566182*    6224*
```

* means statistics collection is not supported by one or more of the line cards.

History

Release version	Command history
5.4.00	This command is modified to include the parameters **transit**, **fec**, and *ip_addr* .

show mpls statistics ldp tunnel

Displays the total combined statistics of all ECMP paths of an LDP tunnel with LDP ECMP LER feature.

Syntax

show mpls statistics ldp tunnel [*dec* | *vif-index*]

Parameters

dec

Specifies the destination prefix.

vif-index

Displays the total combined statistics of all ECMP paths of an LDP tunnel with LDP ECMP LER feature.

Modes

User EXEC mode

Usage Guidelines

The statistics are not accurate when the system runs out of CAM entries for all the ECMP paths.

Command Output

The **show mpls statistics ldp tunnel** command displays the following information:

Output field	Description
LSP	The name of the LSP that statistics are being displayed for (displayed for RSVP-signaled LSPs only).
tnl	The index number of the MPLS tunnel
pkt	The total number of packets forwarded through the specified LSP.
Byte	The total number of bytes forwarded through the specified LSP.
Avg. pps	The number of packets-per-second forwarded through the specified LSP.
Avg. Bps	The number of bytes-per-second forwarded through the specified LSP.

Examples

The following example shows the output of the **show mpls statistics ldp tunnel** command.

```
device# show mpls statistics ldp tunnel
LDP tunnel interface tn113  0 pkt  0 Byte  0 Avg. pps  0 Avg. Bps
```

History

Release Version	Command history
5.5.00	This command was modified to show the total combined statistics of all ECMP paths of an LDP tunnel with the LDP ECMP LER feature.

show mpls statistics lsp

Displays ingress tunnel accounting for RSVP-signaled LSPs.

Syntax

show mpls statistics lsp [*lsp_name*]

Parameters

lsp_name

Displays statistics for a specified LSP.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays output from the **show mpls statistics lsp** command:

```
device# show mpls statistics lsp
LSP tope4
 Tunnel index 0 0 pkt 0 Byte 0 Avg. pps 0 Avg. Bps
LSP 400
 Tunnel index 2 0 pkt 0 Byte 0 Avg. pps 0 Avg. Bps
LSP 4000
 Tunnel index 3 0 pkt 0 Byte 0 Avg. pps 0 Avg. Bps
LSP tope41
 Tunnel index 4 99205408 pkt 11314220016 Byte 84459 pps 9628340 Bps
```

show mpls statistics oam

Displays OAM MPLS statistics.

Syntax

show mpls statistics oam

Modes

User EXEC mode.

Usage Guidelines

Use the **show mpls statistics oam** command to display the following LSP ping and traceroute counters:

- Ping and traceroute requests that are issued by the user
- Echo requests sent
- Echo requests received
- Echo request time-outs
- Echo replies sent
- Echo replies received
- Echo replies with error return codes

The **clear mpls statistics oam** command clears the LSP ping and traceroute counters.

Examples

The following example displays the output of the **show mpls statistics oam** command.

```
device # show mpls statistics oam
User ping request processed: 8
User traceroute request processed: 3
Echo requests: sent(102658), received(2865), timeout(0)
Echo replies: sent(2865), received(102628)
Echo reply return code distribution: TX RX
Egress(3) : 0 102628
Transit(8) : 0 0
No return code(0) : 0 0
Malformed request(1) : 0 0
Unsupported TLV(2) : 2865 0
No FEC mapping(4) : 0 0
DS map mismatch(5) : 0 0
Unknown upstream intf(6) : 0 0
Reserved return code(7) : 0 0
Unlabeled output intf(9) : 0 0
FEC mapping mismatch(10) : 0 0
No label entry(11) : 0 0
Rx intf protocol mismatch(12) : 0 0
Premature LSP termination(13) : 0 0
```

show mpls statistics vll

Displays VLL endpoint traffic statistics to see the forwarding counters for each VLL configured on the system.

Syntax

show mpls statistics vll [*vll-id* **extended-counters** | *vll_name* **extended-counters**]

Parameters

vll_id

Specifies the identifier of a VLL instance.

vll_name

Specifies the configured name for a VLL instance.

extended-counters

Displays extended counter (Generation 2 and 3a modules only).

Modes

User EXEC mode.

Command Output

The **show mpls statistics vll** command displays the following information:

Output field	Description
VLL-Name	The configured name of the VLL instance.
VLL-Ports	The port where the traffic is monitored.
VLL-ingress-Pkts	Packets arriving from the Customer Endpoint.
VLL-Egress-Pkts	Packets arriving from the MPLS core and going to the customer interface.

Examples

The following example displays output of all VLL traffic statistics on a Brocade device.

```
device# show mpls statistics vll
VLL-name    VLL-Ports    VLL-Ingress-Pkts    VLL-Egress-Pkts
--------    ---------    ----------------    ---------------
VLL1        e1/1         100                 100
VLL2        e1/4         100                 100
```

NOTE

The VLL name repeats for each module where the statistics are collected and display on the Management console.

The following example shows the output of VLL traffic statistics for a VLL instance, specified by its VLL name.

```
device# show mpls statistics vll vll1
VLL-Name    VLL-Ports    VLL-Ingress-Pkts    VLL-Egress-Pkts
--------    ---------    ----------------    ---------------
VLL1        e1/1         100                 100
```

The following example shows the output of VLL traffic statistics for a VLL specified, by its VLL ID.

```
device# show mpls statistics vll 4
VLL-Name    VLL-Ports    VLL-Ingress-Pkts    VLL-Egress-Pkts
--------    ---------    ----------------    ---------------
VLL1        e1/1         100                 100
```

show mpls statistics vll-local

When extended counters are enabled, displays the number of bytes and packets received and sent on a particular endpoint or all endpoints of that Local VLL instance.

Syntax

show mpls statistics local-vll [*vll_name* | *vll_id* [**extended-counters** [[**vlan** *vlan_id*] [**ethernet** *port_id*]]]]

Parameters

vll_name

Specifies the configured name for the Local VLL instance.

vll_id

Specifies the ID of a Local VLL instance.

extended-counters

Enables the extend counters for a particular Local VLL instance.

vlan *vlan_id*

Specifies the ID of the configured VLAN.

ethernet *port_id*

Specifies the Ethernet port.

Modes

User EXEC mode.

Usage Guidelines

clear mpls statistics vll-local

Command Output

The **show mpls statistics vll-local** command with the **extended-counters** option displays the following information:

Output field	Description
VLL	The configured name for a Local VLL instance.
VLL-ID	The ID of the Local VLL instance.
VLAN	The ID of the configured VLAN.
Port	The port ID of the interface for which the user wants to display the counters.
RxPkts	The number of packets received at the specified port.
TxPkts	The number of packets transmitted from the specified port.
RxBytes	The number of bytes received at the specified port.
TxBytes	The number of bytes transmitted from the specified port.

Examples

The following example displays the output of the **show mpls statistics vll-local** command with the **extended-counters** option:

```
device# show mpls statistics vll-local loc8 extended-counters
VLL loc8, VLL-ID9:Extended Counters (only applicable for G2 modules)
VLAN    Port    RxPkts   TxPkts    Rxbytes     TxBytes
94      5/2     4639941  0         1187824896  0
        p0      0        0         0           0
        p1      0        0         0           0
        p2      0        0         0           0
        p3      0        0         0           0
        p4      4639941  0         1187824896  0
        p5      0        0         0           0
        p6      0        0         0           0
        p7      0        0         0           0
```

When the per-VLAN, port, and priority-based accounting mode is disabled, the following output is displays for the **show mpls statistics vll-local** command with the **extended-counters** option:

```
device# show mpls statistics vll-local loc8 extended-counters
VLL loc8, VLL-ID9:Extended Counters (only applicable for G2 modules)
VLAN    Port    RxPkts    TxPkts    Rxbytes    TxBytes
94      5/2     1175769   0         300996864  0
92      8/2     0         1178559   0          301711104
```

show mpls statistics vpls

Displays statistics based on VPLSs.

Syntax

show mpls statistics vpls [*vpls_id* | *vpls_name*]

show mpls statistics vpls { *vpls_id* | *vpls_name* } **extended-counters vlan** *vlan_id* [**detail** | **routed** | **switched**]

show mpls statistics vpls { *vpls_id* | *vpls_name* } **extended-counters vlan** *vlan_id* [**inner-vlan** *inner_vlan_id*] [**ethernet** *slot* **/** *port*] [**detail** | **routed** | **switched**]

Parameters

vpls_id
Displays specified VPLS by numerical ID.

vpls_name
Displays specified VPLS by name.

vlan *vlan_id*
Displays Extended Counters for end points of a VPLS VLAN (single tag only).

extended-counters
Displays Extended Counters (G2/G3 modules only).

detail
Displays Extended Counters in a detailed format.

routed
Displays Extended Counters for routed packets.

switched
Displays Extended Counters for switched packets.

inner-vlan *inner_vlan_id*
Specifies the ID of the configured inner VLAN.

ethernet *slot* **/** *port*
Displays Extended Counters for a VPLS endpoint.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the **show mpls statistics vpls** command with the **extended-counters detail** option.

```
device#show mpls statistics vpls 1 extended-counters detail
VPLS Extended Counters (only applicable for G2 modules):
VPLS Name: a, VPLS  Id: 1

VPLS Vlan: vlan 100
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 4/1
 Routed   0                0                0                0
 Switched 6525316          15195085         574227808        1337167480
 Combined 6525316          15195085         574227808        1337167480

VPLS Vlan: vlan 200
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 4/8
 Routed   0                0                0                0
 Switched 17084263         5845698          1503415144       514421424
 Combined 17084263         5845698          1503415144       514421424
```

The following example displays the **show mpls statistics vpls** command with the **extended-counters routed** option.

```
device#show mpls statistics vpls 1 extended-counters routed
VPLS Extended Counters (only applicable for G2 modules):
VPLS Name: a, VPLS  Id: 1

VPLS Vlan: vlan 100
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 4/1   0                0                0                0

VPLS Vlan: vlan 200
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 4/8   0                0                0                0
```

The following example displays the **show mpls statistics vpls** command with the **extend-counters switched** option.

```
device#show mpls statistics vpls 1 extended-counters switched
VPLS Extended Counters (only applicable for G2 modules):
VPLS Name: a, VPLS  Id: 1

VPLS Vlan: vlan 100
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 4/1   6525316          15195085         574227808        1337167480

VPLS Vlan: vlan 200
Interface RxPkts           TxPkts           RxBytes          TxBytes
eth 4/8   17084263         5845698          1503415144       514421424
```

History

Release version	Command history
5.4.00	This command was modified to display MPLS routed and switched statistics. Use this command to get statistics per VLAN and per interface, either routed or switched. This is available for only Gen2 cards.
5.9.00	This command was modified to include the **inner-vlan** *vlan_id* parameter.

show mpls statistics vrf

Displays statistics based on Virtual Routing and Forwarding (VRF)s.

Syntax

show mpls statistics vrf *vrf_name*

Parameters

vrf_name

Displays specified VRF by name.

Modes

User EXEC mode

Usage Guidelines

Command Output

The **show mpls statistics vrf** command displays the following information:

Output field	Description
VRF Name	The name of the VRF from which packets originated or are destined.
In-Port(s)	The port that is either the VRF or MPLS interface.
Endpt Out-Pkt	The number of packets forwarded to the specified VRF interface.
Tnl Out-Pkt	The number of VRF data packets sent to the remote peer over an MPLS tunnel.

Examples

The following example displays out-packet statistics for VRFs.

```
device# show mpls statistics vrf
VRF Name In-Port(s) Endpt Out-Pkt Tnl Out-Pkt
red e3/1 0 0
e3/2 0 0
e3/3 0 0
e3/4 0 0
e5/1 - e5/10 0 0
e5/11 - e5/20 0 0
e5/21 - e5/30 0 0
e5/31 - e5/40 0 0
green e3/1 3707480 0
e3/2 2692915 0
e3/3 0 0
e3/4 0 0
e5/1 - e5/10 0 0
e5/11 - e5/20 0 5834179
e5/21 - e5/30 0 0
e5/31 - e5/40 0 0
pink e3/1 0 0
e3/2 0 0
e3/3 0 0
e3/4 0 0
e5/1 - e5/10 0 0
e5/11 - e5/20 0 0
e5/21 - e5/30 0 0
e5/31 - e5/40 0 0
```

The following example displays out-packet statistics for a specific VRF.

```
device# show mpls statistics vrf black
VRF Name In-Port(s) Endpt Out-Pkt Tnl Out-Pkt
black e3/1 0 0
e3/2 29607351 0
e3/3 27522998 25828420
e3/4 0 0
e5/1 - e5/10 0 0
e5/11 - e5/20 0 0
e5/21 - e5/30 0 0
e5/31 - e5/40 0 0
e5/31 - e5/40 0
```

show mpls summary

Displays a summary of MPLS information, including the number of configured paths and signaled LSPs for which this device is the ingress LSR.

show mpls summary

summary

Displays MPLS global counters.

User EXEC mode

The **show mpls summary** command output has additional information on the total number of bypass LSPs in the system. This total number is the sum of the configured static and dynamic bypasses in the system.

The **show mpls summary** command displays the following information:

Output field	Description
Transit-LSPs configured	The number of static LSP transits configured.
Transit-LSPs enabled	The number of static LSP transits enabled.
Transit-LSPs operational	The number of static LSP transits operational.

The following example displays the output of the **show mpls summary** command.

```
device# show mpls summary
CER40 (config-mpls-lsp-test)#show mpls summary
Path:
        Paths configured          =     2

RSVP-Signaled LSPs:
        LSPs configured           =     6
        LSPs enabled              =     6
        LSPs operational          =     6
        Detour LSPs UP            =     0
        Backup LSPs UP            =     0
        Bypass LSPs               =     0
        Bypass LSPs UP            =     0
        Bypass LSPs enabled       =     0

LDP-Signaled LSPs:
        LSPs operational          =     3
…
Number of times MPLS has been enabled: 1
Next available RSVP LSP tunnel-interface index: 7
```

Release version	Command history
5.9.00	This command was modified to include the next available RSVP LSP tunnel-interface index.

show mpls ted database

Displays the contents of an LSR TED.

Syntax

show mpls ted database [*node_id* **detail** | **detail** *node_id*]

Parameters

node_id **detail**

Displays the detailed node identification information.

detail *node_id*

Displays the detailed information of the Traffic Engineering Database (TED) content specified by the *node_id* variable.

Modes

User EXEC mode.

Command Output

The **show mpls ted database** command displays the following information:

Output field	Description
AreaID	The identification of this OSPF area.
NodeID	The identification of the node. For router nodes, can be any interface address or a loopback interface address on the LER. For network nodes, this is the router identification of the network's designated router.
(node) Type	The node type can be either 'Router' or 'Network'. • 'Router' indicates the node is an actual LSR. • 'Network' indicates the node represents a multi-access network.
(link) Type	The link type can be either 'P2P' or 'M/A'. • 'P2P' indicates this is a point-to-point link. • 'M/A' indicates the link is a broadcast, multi-access network.
To	The identification of the node at the end of the link.
Local	The address of the interface used to reach the remote node.
Remote	The address of the interface on the remote node that connects to the local node. For M/A types, this is always 0.0.0.0.

Examples

The following example displays the output of the **show mpls ted database** command.

```
device# show mpls ted database
AreaID: 0
 NodeID: 2.2.2.2, Type: Router
  Type: M/A, To: 10.1.1.2, Remote: 0.0.0.0
 NodeID: 3.3.3.3, type: Router
  Type: P2P, To: 10.1.1.2, Local: 10.1.1.1, Remote: 10.1.1.2
  Type: M/A, To: 10.1.1.3, Local: 10.1.1.3, Remote: 0.0.0.0
  Type: M/A, To: 10.1.1.2, Local: 10.1.1.1, Remote: 0.0.0.0
 NodeID: 10.1.1.3, Type: Network
  Type: M/A, To: 10.1.1.1, Local: 0.0.0.0, Remote: 0.0.0.0
  Type: M/A, To: 10.2.2.2, Local: 0.0.0.0, Remote: 0.0.0.0
  Type: M/A, To: 10.3.3.3, Local: 0.0.0.0, Remote: 0.0.0.0
 NodeID: 30.1.1.2, type: Network
  Type: M/A, To: 10.1.1.1, Local: 0.0.0.0, Remote: 0.0.0.0
  Type: M/A, To: 10.6.6.6, Local: 0.0.0.0, Remote: 0.0.0.0
```

show mpls ted path

Displays a traffic path to an IPv4 destination address using a specified set of resource parameters.

Syntax

show mpls ted path { *ip_addr* } [**bandwidth** *kbps*] [**cspf-comp-mode** { **use-igp-metric** | **use-te-metric** }] [**exclude-any** *name*] [**hop-limit** *max_hops*] [**include-all** *name*] [**include-any** *name*] [**path-name** *name*] [**priority** *setup*] [**tie-breaking** { **least-fill** | **most-fill** | **random** }]

Parameters

ip_addr

The IPv4 address of the destination host.

bandwidth

The minimum bandwidth of the path to its destination.

kbps

Enter the bandwidth value in decimal form for kilobits per second units. The valid range is between 0 - 2147483647. When the value entered is larger than 2147483647, then the value is truncated to the max limit of 2147483647 and accepted as the bandwidth input.

cspf-comp-mode

Selects CSPF computation mode to use to calculate the path.

use-igp-metric

Selects igp-metric to calculate the path.

use-te-metric

Selects te-metric to calculate the path.

exclude-any

Excludes any of the administrative groups.

name

Selects the list of administrative groups to exclude. A list of any combination of administrative groups names or numbers. The valid range for the administrative group number is between 0 - 31. The administrative group name must start with an alphabet character. When entering an invalid range for an administrative group number or name, the CLI prompts a warning message, and then the CLI prompts a warning message. It accepts the CLI but ignores the out of range value.

hop-limit

The *maximum* number of hops for the path to reach its destination.

max-hops

The valid range is between 0 - 255. When an invalid range is entered, an error message displays. When a path to the destination is available, but the hop count for the path is greater than the *max_hops* value, then MPLS indicates that the path is not available.

include-all

Includes all of the administrative groups.

name

Selects the list of administrative groups. A list of any combination of administrative groups names or numbers. The valid range for the administrative group number is between 0 - 31. The administrative group name must start with an alphabet character. When an invalid range is entered for an administrative group number or name, then the CLI prompts a warning message, the CLI prompts a warning message. The CLI is accepted, but the out of range value is ignored.

path

Displays by path name.

name

Name of selected path.

priority

The setup priority of the path.

setup

The valid range is between 0 - 7. The default is 7, the *lowest* setup priority value. When an invalid range is entered, an error message displays. The priority parameter must be entered along with the bandwidth parameter because while setting up an LSP, the setup priority value decides the ability to reserve a bandwidth amount.

tie-breaking

Use when multiple equal-cost paths to a destination exist. The tie-breaking rule selects only one path to display from among multiple equal cost paths. The default is random.

least-fill

Path is selected on least-fill criteria.

most-fill

Path is selected on most-fill criteria.

random

Path is selected randomly.

Modes

User EXEC mode

Usage Guidelines

Command Output

The **show mpls ted path** command displays the following information:

Output field	Description
Path to *x.x.x.x* found	The IPv4 address of the destination host is found.
Time taken to compute	The total time taken by CSPF (in milliseconds) to compute this path.
Hop-count	The hop count of this path.
Cost	The total cost of this path.
IS-IS	The IS-IS or OSPF or CSPF area ID through which this path traverses.

Output field	Description
Hop	The ingress interface IPv4 address at each top.
Rtr	The traffic engineering router ID (IPv4 address) at each hop.

Examples

The following example displays the **show mpls ted path** command.

```
device# show mpls ted path 10.12.12.12. hop-limit 2
Path to 10.12.12.12. found! Time taken to compute: 0 msec
Hop-count: 2 Cost: 2000 ISIS Level-1
         Hop 1: 10.1.0.1, Rtr 10.13.13.13
         Hop 2: 10.1.0.2, Rtr 10.12.12.12
```

The following example displays the **show mpls ted path** command for a router where the **exclude-any** parameter is used.

```
device# show mpls ted path 10.11.11.11 exclude-any 0
Path to 10.12.12.12. found! Time taken to compute: 0 msec
Hop-count: 1 Cost: 10 ISIS Level-2
        Hop 1: 10.0.0.13, Rtr 10.11.11.11
```

The following example displays the **show mpls ted path** command using the **hop-limit** parameter when entering an out-of-range parameter value.

```
device# show mpls ted path 10.2.2.2 hop-limit 300
Error- Hop count value is out of range [0-255]
```

When entering an out-of-range parameter value, the following error message displays for the priority parameter:

```
Priority
```

show mpls vll

Displays detailed information about the configurations of the Virtual Leased Lines (VLLs) on the device.

Syntax

show mpls vll [*vll_id* | *vll_name*] [**detail**] [**redundancy**]

show mpls vll brief [**redundancy**]

Parameters

vll_id
Displays the selected VLL by ID.

vll_name
Displays the selected named VLL by name.

detail
Displays detailed information of the named VLL.

redundancy
Displays MCT VLLs and VLLs having redundant peers.

brief
Displays brief information of the named VLL.

Modes

User EXEC mode

Usage Guidelines

The **show mpls vll detail** command displays information about the operational state of the VPLS instance regarding the local endpoints.

Command Output

The **show mpls vll detail** command displays the following information:

Output field	Description
End-point	How packets forward once they reach the egress LER. It can be one of the following: • "untagged *portnum* " - Forward the packet out the specified port as untagged. • "tagged vlan *vlan_id* / *portnum* " - Tag the packet with the specified VLAN ID and forward the packet out the specified port. • "tagged vlan *vlan_id* inner-vlan *vlan_id* " - Tag the packet with the specified outer and inner vlan IDs and forward the packet out the specified port • "undefined" - An endpoint has not been configured for this VLL.
End-point state	The current state of the VLL. It can be one of the following: • "UP" VLL is operational - packets can flow

Output field	Description
	• "DOWN - configuration incomplete" A required configuration statement is missing. • "DOWN - endpoint port to CE is down" The physical endpoint port that must connect to the Customer Edge device is down, due to a link outage or it is administratively disabled. • "DOWN - no tunnel LSP to vll-peer" cannot find a working LSP. • "DOWN - PW is Down (Reason: LDP session is down)" LDP session is not yet ready. • "DOWN - Waiting for PW Up" VLL is waiting for MPLS to bring up the session. • "DOWN - Waiting for VC withdrawal Completion" PW is down, and VLL is waiting for MPLS to withdraw the labels that VLL has requested. • "DOWN - PW is Down (Reason: Out of VC labels)" PW is down; VC labels are not available. • "DOWN - PW is Down (Reason: Out of Memory)" PW is down; there is not sufficient memory available. • "DOWN - PW is Down (Reason: Waiting for Remote VC label)" PW is down; waiting for remote peer's VC label to advertise. • "DOWN - waiting for VC label binding from vll-peer" The device has advertised its VC label binding to the VLL peer but has not yet received the peer's VC label binding. • "DOWN - PW is Down (Reason: MTU mismatch Local- MTU *mtu-value* , Remote-MTU mtu-value)" PW is down, and the MTU values for the local and remote peers are not equal. • "DOWN - PW is Down (Reason: VC type mismatch, Local VC type: *vc-type* , Remote VC type: *vc-type* " - The session cannot be come up because the VC types of the local and remote peers are not equal. The possible value for the *vc-type* variable is five (5) for raw mode or four (4) for tagged mode.
MCT state	Options: Active, Passive, NC
IFL-ID	The Internal Forwarding Lookup Identifier (IFL-ID) allocation to each Local VLL instance that has, at least, one dual-tagged endpoint. For instances that do not have dual-tagged endpoints, the IFL-ID is displayed as "--".
Local VC type	Indicates whether the local VC is in raw-mode or tagged-mode.
Local VC MTU	The MTU value configured for this local VC.
COS	The optional CoS setting for the VLL. When a CoS value sets, the device attempts to select a tunnel LSP that also has this CoS value. The CoS value can be from 0 through 7.
Extended Counters	Indicates whether or not the extended counters are enabled for the configured VLL.
Vll-Peer	The remote PE router. It must be the same as the LSP destination for the LSPs that the VLL transports over.
State	The current state of the VLL. It can be either UP or DOWN. Data can be forwarded over the VLL only when the state is UP.
Remote VC type	Indicates whether the remote VC is in raw mode or tagged mode.
Remote VC MTU	The MTU value advertised from the VLL peer.
Local label	The VC label value locally allocated for this VLL. Packets forwarded from the VLL peer to this device are expected to contain this label. It is the label that is advertised to the VLL peer through LDP.
Remote label	The VC label allocated by the VLL peer and advertised to this device through LDP. The device applies this label to outbound MPLS packets sent to the VLL peer.
Local group-id	The VLL group ID (defined in draft-martini-l2circuit-trans-mpls-07.txt) advertised to the VLL peer through LDP. The group ID is always zero.
Remote group-id	The VLL group ID selected and advertised by the VLL peer.
Tunnel LSP	The name, as well as the internal tunnel index number, of the tunnel LSP selected for the VLL.

Output field	Description
MCT Status TLV	Options: • Active - Node will start peering with the remote peers, signaling Status TLV as Active. • Standby - Node will start peering with remote peers, signaling Status TLV as Standby. • Transit - MCT VLL is not in the operational state. Remote peering is not yet enabled.
LSPs assigned	Lists the assigned LSPs.

Examples

The following example displays the detailed information about the VLL.

```
device# show mpls vll detail

VLL VLL_to_R3, VC-ID 40000, VLL-INDEX 1

  End-point        : untagged  e 1/7
  End-Point state  : Up
  MCT state        : None
  IFL-ID           : --
  Local VC type    : tag
  Local VC MTU     : 1500
  COS              : --
  Extended Counters: Enabled

  Vll-Peer         : 192.168.2.102
    State          : UP
    Remote VC type : tag              Remote VC MTU  : 1500
    Local label    : 851968           Remote label   : 851968
    Local group-id : 0                Remote group-id: 0
    load balance   : enable
    number of tunnels : 8
    Tunnel LSP     : tnl0[RSVP],tnl1[RSVP]),tnl2[RSVP],tnl3[RSVP],
                     tnl4[RSVP],tnl5[RSVP],tnl6[RSVP],tnl7[RSVP]
    MCT Status TLV : --
    LSPs assigned  : No LSPs assigned
```

History

Release version	Command history
5.5.0	A new addition in the **detail** option was added to allow the user to select raw pass-through mode. The option behaves like tagged mode when the endpoint is configured as a tagged endpoint or raw mode when the endpoint is configured as an untagged endpoint.
5.7.0	This command was modified to include the "LSP assigned" field in the display output for **show mpls vll detail**, **show mpls vll** *vll_name* , and **show mpls vll** *vll_id* .
6.0.0	This command was modified to show whether load balancing is enabled, and the number of tunnels.

show mpls vll-local

Displays information about individual Local VLLs configured on the router.

Syntax

show mpls vll-local *local_vll_name* [**brief** | **detail**]

Parameters

local_vll_name

Specifies the local VLL name.

brief

Displays brief information.

detail

Displays detailed information for all local VLLs in the router. Specifying a particular VLL using the *vll-name* option limits the display to the specified Local VLL.

Modes

User EXEC mode.

Command Output

The **show mpls vll-local** command displays the following information:

Output field	Description	Command level
Name	The configured name of the Local VLL.	show mpls vll-local
VLL-ID	The VLL ID.	show mpls vll-local
End-point	How packets forward out of the egress port of the Local VLL. This can be one of the following: • '**untagged portnum**' - Forward the packet out the specified port as untagged. • '**tag vlan vlan_id/portnum**' - Tag the packet with the specified VLAN ID and forward the packet out the specified port. • '**undefined**' - An endpoint has not been configured for this Local VLL. • '**inner-vlan**' - describes the inner-vlan tag for an end-point that is configured for dual-tagging.	show mpls vll-local show mpls vll-local detail
IFL-ID	The *Internal Forwarding Lookup Identifier (IFL-ID)* allocated to each Local VLL instance that has at least one dual tag endpoint. For instances that do not have dual tag endpoints, the IFL-ID is displayed as '-'.	show mpls vll-local detail

Output field	Description	Command level
State	The current state of the Local VLL. It can be one of the following: • 'UP'- The local VLL is operational - packets can flow. • 'DOWN - configuration complete' - A required configuration statement is missing. • 'DOWN - endpoint port is down' - The physical endpoint port is down due to a link outage or is administratively disabled.	show mpls vll-local show mpls vll-local detail
COS	The optional CoS setting for the Local VLL. When a CoS value sets, the CoS value can be between 0 - 7.	show mpls vll-local detail
Extended Counters	Indicates whether or not the extended counters are enabled for the configured Local VLL instances.	show mpls vll-local detail

Examples

The following example shows the output of the **show mpls vll-local** command:

```
device# show mpls vll-local
Name         VLL-ID    End-point1                      End-point2         State
foundrylong  1         tag vlan 100 e5/12              undefined          DOWN
villocalfou
ndrylonfvll
localfoundr
ylongvilloc
alfoundry
test         2         tag vlan 200 inner-vlan 50 e2/1  tag vlan 200 e2/2  UP
```

The following example shows detailed information for all Local VLLs in the router. Using the *vll_name* option limits the display to the specified Local VLL.

```
device# show mpls vll-local detail
VLL-test-1    VLL-ID1     IFL-ID-      State:UP
End-point1:untagged e2/2                    COS:-
End-point2:untagged e2/13                   COS:-  Extended Counters:Enabled

VLL-test-2    VLL-ID2     IFL-ID-      State:UP
End-point1:tagged vlan 2500 e2/10           COS:-
End-point2:tagged vlan 2500 e2/9            COS:-  Extended Counters:Enabled

VLL-test-3    VLL-ID3     IFL-ID-      State:UP
End-point1:tagged vlan 2501 e2/10           COS:6
End-point2:tagged vlan 2501 e2/9            COS:5  Extended Counters:Enabled

VLL-test-4    VLL-ID4     IFL-ID4096   state:UP
End-point1:tagged vlan 100 inner-vlan 45 e2/1  COS:-
End-point2:tagged vlan 100 e2/3             COS:-  Extended Counters:Enabled
```

show mpls vpls

Displays information about the VPLS configuration.

Syntax

show mpls vpls [**brief** [**redundancy**] | **detail** | **down** | **id** *vpls_id* | **local** | **name** *vpls_name* | **summary**]

Parameters

brief

Displays brief information for each VPLS (default).

redundancy

Displays cluster-peer pw redundancy.

detail

Displays detailed information for each VPLS.

down

Displays brief information for each VPLS that is not completely operational.

id *vpls_id*

Displays detailed information for the VPLS specified by its ID.

local

Displays detailed information for local entry.

name *vpls_name*

Displays detailed information for the VPLS specified by its name.

summary

Displays summary information.

Modes

User EXEC mode

Usage Guidelines

When both the VC type and MTU are mismatched, only the output from the VC type mismatch is displayed on the console.

This command operates in all modes.

Command Output

show mpls vplsdetail

Output field	Description
VPLS	The configured name of the VPLS instance.
Max mac entries	The maximum number of MAC entries that can be learned for the VPLS instance.

Output field	Description
Total vlans	The number of VLANs that are translated for this VPLS instance.
Tagged ports	The total number of tagged ports that are associated with VLANs in this VPLS instance, as well as the number of these ports that are up.
Untagged ports	The total number of untagged ports that are associated with VLANs in this VPLS instance, as well as the number of these ports that are up.
IFL-ID	The Internal Forwarding Lookup Identifier (IFL-ID) for dual-tagged ports in the VPLS instance.
L2 Protocol	Layer 2 control protocol configured on the VLAN.
Tagged	The numbers of the tagged ports in each VLAN.
VC-Mode	The VC mode for the VPLS instance. • **Raw** - The VLAN tag information in the original payload is not carried across the MPLS cloud. • **Tagged** - The VLAN tag information in the original payload is carried across the MPLS cloud. • **Raw pass-through** - The VLAN tag information behaves like tagged mode when all endpoints are configured as tagged endpoints.
Total VPLS peers	The number of VPLS peers this device has for this VPLS instance, as well as the number of these VPLS peers with which this device has an LDP session.
Peer address	The IP address of the VPLS peer.
State	The current state of the connection with the VPLS peer. This can be one of the following states: • **Operational** - The VPLS instance is operational. Packets can flow between the device and the peer. • **Wait for functional local ports** - The physical endpoint port that must be connected to the Customer Edge device is down due to a link outage or is administratively disabled. • **Wait for LSP tunnel to Peer** - The device cannot find a working tunnel LSP. • **Wait or PW Up (Wait for LDP session to Peer)** - The LDP session is not ready. • **Wait for PW Up (Wait for remote VC label)** - The device has advertised its VC label binding to the VPLS peer, but has not yet received the peer's VC labeling binding. • **Wait for PW Up (VC type mismatched)** - A session is not formed because the VC type does not match with its peer's VC type. • **Wait for PW Up (MTU mismatched)** - The MTU sent to a peer is derived from the device's global setting by the following formula: (system-mtu minus 26 bytes). When a system-mtu value is not configured, a default value of 1500 is sent. • **Wait for PW Up (Wait for LDP session to Peer)** - The LDP session to the peer is down. • **Wait for PW Up (No label resource)** - When configuring a VPLS peer, the maximum number of VC labels that can be supported may exceed 65536 and cause the configuration to be rejected. The maximum number of VC labels available for VPLS instances is equal to 65536.
Uptime	The time, in minutes, that the entry has been operational.
Tnnls in use (load balance)	The tunnel LSP used to reach the VPLS peer. When VPLS traffic to the peer is load balanced across multiple tunnel LSPs, the tunnel LSPs used to reach the peer are displayed.
Local VC lbl	The VC label value locally allocated for this peer for this VPLS instance. Packets forwarded from the VPLS peer to this device are expected to contain this label. This is the label that is advertised to the VPLS peer through LDP.
Remote VC lbl	The VC label allocated by the VPLS peer and advertised to this device through LDP. The device applies this label to outbound MPLS packets sent to the VPLS peer.
Local VC MTU	The MTU value locally configured for this peer.
Remote VC MTU	The MTU value configured for the remote VPLS peer.
Local VC-Type	The VC type for this peer.
Remote VC-Type	The VC type for the remote VPLS peer.

Output field	Description
CPU-Protection	Whether CPU protection configured on this VPLS instance is on or off. On Brocade NetIron XMR Series and Brocade NetIron MLX Series devices only: When CPU protection is enabled on this VPLS instance but is temporarily unavailable due to 100% multicast FID usage, this field includes the message shown above.
Local Switching	Whether local switching behavior on a per-VPLS basis is enabled or disabled.
Extended Counter	Indicates whether or not the extended counter is enabled for the configured VPLS.
Multicast Snooping	Indicates whether multicast snooping is enabled or disabled.

Examples

The following example displays the output of the **show mpls vpls brief redundancy** command.

```
device# show mpls vpls brief redundancy
                Ports   Num    Peers   MCT      MCT FSM
Name    Id      Up      Peers  Up      PW-Role  State
====    ==      =====   =====  =====   ======   ====
tst     10      2       2      2       Active   OPER
```

The following example displays the output of the **show mpls vpls detail** command.

```
device# show mpls vpls detail
VPLS 1001, Id 1001, Max mac entries: 32000
 Total vlans: 2, Tagged ports: 1 (1 Up), Untagged ports 0 (0 Up)
 IFL-ID: 4096
  Vlan 1001
   Tagged: ethe 14/3
  Vlan 1001 inner-vlan 1001
   Tagged: ethe 14/3
 VC-Mode: Raw
 Total VPLS peers: 6 (6 Operational)
 Peer address: 10.0.0.1, State: Operational, Uptime: 1 hr 44 min
  LSPs assigned: f1a1 a1a2 a2a5 a3a8,  Tnnls in use (load balance): Candidate count:1 (only 1st 4 is
displayed):
  tnl0(1217)[RSVP]     Peer Index:0
  Local VC lbl: 983839, Remote VC lbl: 984238
  Local VC MTU: 9190, Remote VC MTU: 9190
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 Peer address: 10.0.0.2, State: Operational, Uptime: 1 hr 44 min
  LSPs assigned: f1b1 a1b2 a2b5 a3b8,  Tnnls in use (load balance): Candidate count:1 (only 1st 4 is
displayed):
  tnl4(1075)[RSVP]     Peer Index:1
  Local VC lbl: 983239, Remote VC lbl: 984238
  Local VC MTU: 9190, Remote VC MTU: 9190
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 Peer address: 10.0.0.3, State: Operational, Uptime: 1 hr 37 min
  LSPs assigned: f1c1 a1c2 a2c5 a3c8,  Tnnls in use (load balance): Candidate count:1 (only 1st 4 is
displayed):
  tnl8(1193)[RSVP]     Peer Index:2
  Local VC lbl: 983439, Remote VC lbl: 983240
  Local VC MTU: 9190, Remote VC MTU: 9190
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 Peer address: 10.0.0.7, State: Operational, Uptime: 1 hr 37 min
  LSPs assigned: f1d1 a1d2 a2d5 a3d8,  Tnnls in use (load balance): Candidate count:1 (only 1st 4 is
displayed):
  tnl12(1355)[RSVP]     Peer Index:3
  Local VC lbl: 984239, Remote VC lbl: 984039
  Local VC MTU: 9190, Remote VC MTU: 9190
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 Peer address: 10.0.0.4, State: Operational, Uptime: 1 hr 44 min
  LSPs assigned: f1e1 a1e2 a2e5 a3e8,  Tnnls in use (load balance): Candidate count:1 (only 1st 4 is
displayed):
  tnl16(1071)[RSVP]     Peer Index:4
  Local VC lbl: 983639, Remote VC lbl: 984238
  Local VC MTU: 9190, Remote VC MTU: 9190
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 Peer address: 10.0.0.6, State: Operational, Uptime: 1 hr 37 min
  LSPs assigned: f1g1 a1g2 a2g5 a3g8,  Tnnls in use (load balance): Candidate count:1 (only 1st 4 is
displayed):
  tnl20(1374)[RSVP]     Peer Index:5
  Local VC lbl: 984439, Remote VC lbl: 983840
  Local VC MTU: 9190, Remote VC MTU: 9190
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 CPU-Protection: OFF
 Local Switching: Enabled
 Extended Counter: ON
 Multicast Snooping: Disabled
```

The following example shows when the remote peer is in an operational state. The total VC labels allocated field no longer displays in the output of the **show mpls vpls id** *vpls_id* command.

```
device# show mpls vpls id 3
VPLS name_raw, Id 3, Max mac entries: 8192
 Total vlans: 1, Tagged ports: 3 (3 Up), Untagged ports 0 (0 Up)
  IFL-ID: 4097
  Vlan 300 inner-vlan 500
   Tagged: ethe 3/1 ethe 3/11 ethe 3/13
 VC-Mode: Raw
 Total VPLS peers: 1 (1 Operational)
 Peer address: 10.200.200.200, State: Operational
, Uptime: 1 hr 10 min
  Tnnl in use: tnl1(4)
  LDP session: Up, Local VC lbl: 983072, Remote VC lbl: 983072
  Local VC MTU: 1500, Remote VC MTU: 1500
  LOCAL VC-Type: Ethernet (0x05), Remote VC-Type: Ethernet (0x05)
 CPU-Protection: OFF
 Local Switching: Enable
```

The following example shows the MCT support for VE over VPLS.

```
device# show mpls vpls id 3
VPLS vevpls, Id 100, Max mac entries: 2048
Routing Interface Id 100
Total vlans: 1, Tagged ports: 1 (1 Up), Untagged ports 0 (0 Up)
IFL-ID: n/a
Vlan 100
 L2 Protocol: NONE
 Tagged: ethe 1/20
VC-Mode: Raw
Total VPLS peers: 2 (2 Operational
Cluster-Peer address: 13.13.13.13, State: Operational, Uptime: 53 sec
 Tnnl in use: tnl0(2049)[RSVP] Peer Index:0
 Local VC lbl: 983042, Remote VC lbl: 983040
 Local VC MTU: 1500, Remote VC MTU: 1500
 Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 9.9.9.9, State: Operational, Uptime: 3 min
 Tnnl in use: tnl1(3)[RSVP] Peer Index:1
 Local VC lbl: 983041, Remote VC lbl: 983040
 Local VC MTU: 1500, Remote VC MTU: 1500
 Local PW preferential Status:Active, Remote PW preferential Status:Active
 Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
CPU-Protection: OFF
Local Switching: Enabled
Extended Counter: ON
Multicast Snooping: Disabled
Cluster-peer: enabled, Role:Active State: VPLS_MCT_STATE_OPER
Vrrp-MCT-aware: enabled
```

The following example displays the output of the **show mpls vpls name** *vpls_name* command.

```
device# show mpls vpls name c1
VPLS c1, Id 10, Max mac entries: 8192
 Total vlans: 0, Tagged ports: 0 (0 Up), Untagged ports 0 (0 Up)
 Total VPLS peers: 1 (0 Operational)
 auto-discovery enabled, RD 10:10
 export RT   10:10
 import RT   10:10
 Peer address: 10.2.2.2 (auto-discovered)
, State: Wait for functional local ports
  Tnnl in use: (load balance)
: None
  LDP session: Up, Local VC lbl: 983040, Remote VC lbl: N/A
  Local VC MTU: 1500, Remote VC MTU: 0
 CPU-Protection: OFF
 Local Switching: Enabled
```

The following example displays the output of the **show mpls vpls summary** command.

```
device# show mpls vpls summary
Virtual Private LAN Service summary:
  Total VPLS configured: 4072, maximum number of VPLS allowed: 4096
  Total number of IFL-ID's allocated by VPLS: 0
  Total VPLS peers configured: 8139, total peers operational: 8138
  Total VPLS Local end-points configured: 0
  Maximum VPLS mac entries allowed: 160000, currently installed: 150530
  VPLS global raw mode VC-Type is Ethernet (0x05)
  VPLS global MTU is 8974, MTU enforcement is OFF
  Global CPU protection: OFF
  VPLS policy parameters:
    vpls-pw-redundancy:  1
  MVIDs in use: 0 of 1 total allocated
  mac-address withdrawal-limit:  500
  MAC age time for local: 300
  MAC age time for remote: 600
```

History

Release version	Command history
5.4.00	This command output was modified to display VPLS instance ID if RSTP is running on a VPLS VLAN. The total VC labels allocated field is no longer displayed in the output of the **show mpls vpls name** *vpls_name* command.
5.5.00	This command was modified to include the **raw pass-through** option for the VC-Mode field. The MAC age time for local and MAC age time for remote fields were added.
5.6.00	VPLS Manual LSP assignment for a peer can now accept a maximum of eight LSPs instead of four LSPs.
5.9.00	The **show mpls vpls summary** command output was modified to include information about the total configured VPLS local endpoints in the system.

show mstp

Displays Multiple Spanning Tree Protocol (MSTP) information.

Syntax

show mstp [**blocked** [*mstp-id* | **region** *region_id*] | *mstp-id* [**region** *region_id*]]

Parameters

blocked

Specifies the display information in respect of ports blocked by the MSTP only.

mstp-id

Specifies the display of information for a specific MSTP instance.

region *region-id*

Specifies the display of information for a specific MSTP region.

blocked

Specifies the display information in respect of ports blocked by the MSTP only.

Modes

User EXEC mode

Usage Guidelines

This command can also be entered in global configuration mode.

History

Release	Command History
5.5.00	The command was modified to display only ports blocked by the Multiple Spanning Tree Protocol.

show mvrp

Displays Multiple VLAN Registration Protocol (MVRP) information.

Syntax

show mvrp [**ethernet** *slot*/*port*]

Parameters

ethernet *slot port*

Displays MVRP information for a specific Ethernet port.

Modes

User EXEC mode

Usage Guidelines

MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Examples

The following example displays MVRP information for all interfaces.

```
device> show mvrp
-----------------------------------------------------------
Total configured mvrp ports     : 2
Global Status                   : Enabled
Join-timer(in ms)               : 200
Leave-timer(in ms)              : 1000
Leaveall-timer(in ms)           : 10000
-----------------------------------------------------------
MVRP Port(s): ethe 1/1 to 1/5, ethe 1/7, ethe 1/9 to 1/11
```

The following example displays MVRP information for Ethernet interface 1/1

```
device> show mvrp ethernet 1/1
-------------------------------------------------------------
MVRP Status                     : Enabled
Join-timer(in ms)               : 200
Leave-timer(in ms)              : 1000
Leaveall-timer(in ms)           : 10000
P2p                             : No
Applicant Mode                  : normal-participant
-------------------------------------------------------------
Registered Vlan(s)              : 1 to 60 77 100 to 500 999
Declared Vlan(s)                : 1 to 60 77 100 to 500 999
Forbidden Vlan(s)               : 10
-------------------------------------------------------------
```

show mvrp attributes

Displays Multiple VLAN Registration Protocol (MVRP) attribute information.

Syntax

show mvrp attributes [**ethernet** *slot*/*port*] [**vlan** *vlan-id*]

Parameters

ethernet *slot port*

Displays MVRP attribute information for a specific Ethernet port.

vlan *vlan-id*

Displays MVRP attribute information for a specific virtual LAN (VLAN).

Modes

User EXEC mode

Usage Guidelines

MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Use this command to display MVRP attribute information for all ports (and optionally, VLANs) that are registered with MVRP on the network. If no keyword options are used, information about all interfaces and VLANs that are registered as MVRP members is displayed.

Examples

The following example displays MVRP attributes for all ports and VLANs.

```
device> show mvrp attributes

Port : 1/1       State : Forwarding
--------------------------------------------------------------------------------
VLAN       Registrar            Registrar            Applicant
           State                Mgmt                 State
--------------------------------------------------------------------------------
11         IN                   FIXED                Very Anxious Observer
12         IN                   FIXED                Very Anxious Observer
Port : 1/2       State : Disabled
--------------------------------------------------------------------------------
VLAN       Registrar            Registrar            Applicant
           State                Mgmt                 State
--------------------------------------------------------------------------------
11         IN                   FIXED                Very Anxious Observer
```

The following example displays MVRP attributes for Ethernet interface 1/1.

```
device> show mvrp attributes ethernet 1/1

Port : 1/1       State : Blocking
-------------------------------------------------------------------------------
VLAN       Registrar           Registrar           Applicant
           State               Mgmt                State
-------------------------------------------------------------------------------
11         IN                  FIXED               Very Anxious Observer
12         IN                  FIXED               Very Anxious Observer
```

The following example displays MVRP attributes for VLAN 11

```
device> show mvrp attributes vlan 100


    ------------------------------------------------------------------------------
PORT  VLAN       Registrar           Registrar          Applicant
                 State               Mgmt               State
-------------------------------------------------------------------------------
1/1   11         IN                  FIXED              Very Anxious Observer
1/2   11         IN                  FIXED              Very Anxious Observer
1/3   11         IN                  FIXED              Very Anxious Observer
```

show mvrp config

Displays Multiple VLAN Registration Protocol (MVRP) configuration information.

Syntax

show mvrp config

Modes

User EXEC mode

Usage Guidelines

MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Use this command to review the MVRP parameters configured on this device.

Examples

The following example displays the MVRP parameters configured on this device.

```
device> show mvrp config

mvrp enable
mvrp timer join 400 leave 2000 leave-all 10000
!
interface ethernet 1/5
  mvrp enable
  mvrp registration-mode forbidden vlan 10
  mvrp timer join 400 leave 1500 leave-all 8000
  mvrp point-to-point
  mvrp applicant-mode non-participant
```

show mvrp statistics

Displays Multiple VLAN Registration Protocol (MVRP) statistics.

Syntax

show mvrp statistics [**ethernet** *slot*/*port*]

Parameters

ethernet *slot port*

Displays MVRP statistics for a specific Ethernet port.

Modes

User EXEC mode

Usage Guidelines

MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Use this command to display MVRP statistics for all ports that are registered with MVRP on the network. If no keyword options are used, statistical information about all interfaces that are registered as MVRP members is displayed.

Examples

The following example displays MVRP statistics for all ports.

```
device> show mvrp statistics

Port  : ethe 1/1
    ------------------------------------------------------------
    Message type                  Received     Transmitted
    ------------------------------------------------------------
    New                           0            0
    In                            0            0
    Join In                       0            0
    Join Empty                    0            0
    Empty                         0            0
    Leave                         0            0
    Leave-all                     0            0
    ------------------------------------------------------------
    Total PDUs                    0            0
    ------------------------------------------------------------
    Port  : ethe 1/2
    ------------------------------------------------------------
    Message type                  Received     Transmitted
    ------------------------------------------------------------
    New                           0            0
    In                            0            0
    Join In                       0            0
    Join Empty                    0            0
    Empty                         0            0
    Leave                         0            0
    Leave-all                     0            0
    ------------------------------------------------------------
    Total PDUs                    0            0
    ------------------------------------------------------------
```

The following example displays MVRP statistics for Ethernet interface 1/1.

```
device> show mvrp statisitcs ethernet 1/1

Port  : ethe 1/1
    ------------------------------------------------------------
    Message type                  Received     Transmitted
    ------------------------------------------------------------
    New                           0            0
    In                            0            0
    Join In                       0            0
    Join Empty                    0            0
    Empty                         0            0
    Leave                         0            0
    Leave-all                     0            0
    ------------------------------------------------------------
    Total PDUs                    0            0
    ------------------------------------------------------------
```

show nht-table ipsec-based

Displays the NHT entries created for IPsec processing.

Syntax

show nht-table ipsec-based

Modes

Privileged EXEC mode

Examples

The following example shows the NHT entries created for IPsec processing.

```
device#show nht-table ipsec-based
Reconcile Done -
      ARP = 0, GRE = 0, MPLS = 0, phase_1 = 0, l2vpn = 0, phase_2 = 0

NHT IP    Index   MAC Address     VLAN    Out I/F  Out Port  TNL CNT XC CNT  LABEL/SPIid     EXP/PCP
1.1.1.2   1       0024.38a5.5130   1        2/1        2/1           1              0             0
device#

device#show nht-table ipsec-based
NHT IP         Index          MAC Address       VLAN        Out I/F  Out Port  LABEL/SPIid   EXP/PCP
1.1.1.2        1            0024.38a5.5130         1         2/1        2/1           0
```

History

Release version	Command history
05.8.00	This command was introduced.

show openflow

Displays the configured OpenFlow parameters.

Syntax

show openflow

Modes

User EXEC mode

Command Output

The **show openflow** command displays the following information:

Output field	Description
Administrative Status	Enable or disable status
Controller Type	OpenFlow 1.0 or OpenFlow 1.3 controller
Controller	Number of controllers

History

Release version	Command history
6.1.00	This command is modified to display the logical ports.
5.7.00	This command was modified for OpenFlow 1.3.
5.5.00	This command was introduced.

show openflow controller

Displays the controller information in a flow.

Syntax

show openflow controller

Modes

User EXEC mode

Command Output

The **show openflow controller** command displays the following information:

Output field	Description
Mode	Gives the active and passive connection of the controller.
IP address	IP address of the port
Port	Port number
Status	After the connection and OpenFlow handshake, the controller gives the role of OpenFlow channel.
Role	Equal, Master and Slave role for the controller.

Examples

The following example displays the results of the **show openflow controller** command.

```
device# show openflow controller
------------------------------------------------------------------------
Contlr Mode  TCP/SSL IP-address     Port       Status            Role
------------------------------------------------------------------------
1   (Equal)    passive  TCP    0.0.0.0          6633   TCP_LISTENING
2   (Master)   active   TCP    10.25.128.179    6633   OPENFLOW_ESABLISHED
3   (Slave)    active   TCP    10.25.128.177    6633   OPENFLOW_ESABLISHED
3   (Equal)    active   TCP    10.25.128.165    6633   OPENFLOW_ESABLISHED
```

History

Release version	Command history
5.5.00	This command was introduced.
5.7.00	This command was modified to give information about the role of the controller.

show openflow flows

Displays the flows information on the OpenFlow ports.

Syntax

show openflow flows

Modes

User EXEC mode

Command Output

The **show openflow flows** command displays the following information:

Output field	Description
Flow	Number of flows
Packet	Total Number of data packets trapped to be sent to controller
Byte	Total Number of data bytes trapped to be sent to controller

Examples

The following example displays the output, when IP section tunnel is down.

```
device# show openflow flows
Total Number of data packets trapped to be sent to controller:                  0
Total Number of data bytes trapped to be sent to controller  :                  0

Total Number of Flows: 1

Flow Id: 8, Priority: 200, FD Id: 0, PW Id: 1
        Rule:
           In Port:      e3/1
           Ether type:   0x00000800

        Meter id: 1
        Action: DROP
                Out Port:       16484[Logical Port]
           FID: -N/A-, MVID: -N/A-
        Hardware Information:
        Port: 3/1   PPCR Id : 6, CAM Index: 0x000840d0 (L4)  PRAM Index: 0x0007ff5b Packets: 29875
        Statistics:
           Total Pkts: 29875
           Total Bytes: 2031500
```

The following example displays the output, when IP section tunnel is up.

```
device# show openflow flows
Total Number of data packets trapped to be sent to controller:                    0
Total Number of data bytes trapped to be sent to controller  :                    0

Total Number of Flows: 1

Flow Id: 8, Priority: 200, FD Id: 0, PW Id: 1
        Rule:
           In Port:      e3/1
           Ether type:   0x00000800

        Meter id: 1
        Action: FORWARD
                Out Port:       16484[Logical Port]
           FID: -N/A-, MVID: -N/A-
        Hardware Information:
        Port: 3/1   PPCR Id : 6, CAM Index: 0x000840d0 (L4)  PRAM Index: 0x0007ff5b Packets: 29875
        Statistics:
           Total Pkts: 29875
           Total Bytes: 2031500
```

History

Release version	Command history
6.1.00	This command was modified to display logical ports.
5.7.00	This command was modified for OpenFlow 1.3.
5.5.00	This command was introduced.

show openflow groups

For a group or a range of groups, displays the maximum number of actions in a bucket, the maximum number of buckets in a group, and the maximum number of groups.

Syntax

show openflow groups [*group-id*]

show openflow groups *group-id* **to** *group-id*

Parameters

groups *group-id*

Displays details of an OpenFlow group or range of groups.

to

Indicates a range of groups.

Modes

User EXEC mode

Command Output

The **show openflow groups** command displays the following information:

Output field	Description
Group	Maximum number of groups in a flow
Bucket	Number of buckets per group
Action	Number of actions per bucket

Examples

The following example displays the output from the **show openflow groups** command.

```
device#show openflow groups
Max number of total groups                          : 512
Max number of total logical groups                   : 128
Max number of buckets per group                     : 64
Max number of buckets per logical groups              : 8
Max number of actions per bucket                    : 1

Max number of groups(ALL/FF/Indirect)               : 512
Max number of buckets per group(ALL/FF/Indirect)    : 64

Max number of SELECT groups                         : 256
Max number of buckets in SELECT group               : 8
Starting Trunk ID for SELECT groups                 : 257


TOTAL number of groups(Type:ALL) in the system      : 0
TOTAL number of groups(Type:FF) in the system       : 0
TOTAL number of groups(Type:Indirect)in the system  : 0
TOTAL number of groups(Type:SELECT) in the system   : 0

TOTAL number of groups in the system                : 0

No groups found
```

The following example displays the output from the **show openflow group group-id** command.

```
device#show openflow group 1

Group id 1

  Status                Active
  Transaction id        4043243760 (0xf0ff00f0)
  Type                  SELECT
  Packet Count          0
  Byte   Count          0
  Flow   Count          0
  Number of buckets     1

  bucket #1
    Weight             1
    Number of actions   1
      action 1: out port: 262145[LSP : abcd]
```

History

Release version	Command history
6.1.00	This command was modified to show logical port information.
5.7.00	This command was introduced.

show openflow interface

Displays the information about the interfaces in a OpenFlow flow.

Syntax

show openflow interface

show openflow interface [**logical** |**physical**]

Modes

User configuration mode

Usage Guidelines

The **show openflow interface** command displays the physical port, up and down links, tag status, MAC addresses, and the modes.

The **show openflow interface logical** command displays enabled OpenFlow logical interfaces information and **show openflow interface physical** displays the physical interfaces.

Command Output

The **show openflow interface** command displays the following information:

Output field	Description
Port	Port Number
Link	Link status
Speed	Configured speed
Tag	Tag status
Mac Address	MAC address of the port
Mode	Gives the information about the layers

Examples

The following example displays information for all OpenFlow interfaces.

```
device# openflow enable layer3 hybrid
device# show openflow interface

Total number of Openflow interfaces: 5

Port  Link     Speed Tag MAC            OF-portid Name    Mode
1/1   Up       1G    Yes 000c.dbf5.bd00 1                 Layer2
1/2   Up       1G    Yes 000c.dbf5.bd01 2                 Layer2
1/3   Up       1G    Yes 000c.dbf5.bd01 3                 Hybrid-Layer3
1/4   Up       1G    Yes 000c.dbf5.bd01 4                 Hybrid-Layer3
1/5   Up       1G    Yes 000c.dbf5.bd01 5                 Hybrid-Layer3
```

The following command displays information for a logical and physical interface.

```
device# show interfaces logical

Total number of Openflow Logical interfaces: 2
Openflow Logical interfaces:
IPSEC-tunnel2        Openflow PORTID:16386      Mode:Hybrid-openflow
IPSEC-tunnel100      Openflow PORTID:16484      Mode:Hybrid-openflow
```

For physical port:

```
device# show openflow interfaces physical
Openflow Physical interfaces:
Port: e3/1      Openflow PortID:97, Mode: Hybrid-Layer23
  Default Drop CAM[CAM:0x00043ffc (V4SACL), PRAM:0x0003ff64, Statistics(Packet): 0]
  Default SA Catchall CAM: --N/A--,DA Catchall CAM: --N/A--
Port: e3/5      Openflow PortID:101, Mode: Hybrid-Layer2
  Default Drop CAM[CAM:0x000440e0 (L4), PRAM:0x0003ff65, Statistics(Packet): 0]
  Default SA Catchall CAM: --N/A--,DA Catchall CAM: --N/A—
```

This command displays OpenFlow enabled interfaces on LP. This command is enhanced to display logical Interface information as well.

```
device# show openflow interfaces
Openflow Physical interfaces:
Port: e3/1      Openflow PortID:97, Mode: Hybrid-Layer23
  Default Drop CAM[CAM:0x00043ffc (V4SACL), PRAM:0x0003ff64, Statistics(Packet): 0]
  Default SA Catchall CAM: --N/A--,DA Catchall CAM: --N/A--
Port: e3/5      Openflow PortID:101, Mode: Hybrid-Layer2
  Default Drop CAM[CAM:0x000440e0 (L4), PRAM:0x0003ff65, Statistics(Packet): 0]
  Default SA Catchall CAM: --N/A--,DA Catchall CAM: --N/A—
Openflow Logical interfaces:
IPSEC-tunnel2        Openflow PORTID:16386      Mode:Hybrid-openflow
IPSEC-tunnel100      Openflow PORTID:16484      Mode:Hybrid-openflow
```

History

Release version	Command history
6.1.00	This command is modified to display logical interfaces.
5.4.00	This command was introduced.

show openflow meters

Displays all the meters in a OpenFlow flow.

Syntax

show openflow meters [*meter-id*]

Parameters

meters *meter-id*

Shows details of a specific OpenFlow meter.

Modes

User EXEC mode

Command Output

The **show openflow meters** command displays the following information:

Output field	Description
Meter-id	Meter number
Band	Number of bands in a meter
Band type	Band type (supported type: Drop, DSCP_REMARK)
Rate	Rate of the band
Counter	Band specific counter

Examples

The following example displays output with specific meter in MP.

```
device(config)# show openflow meters 2
Meter id: 2

  Transaction id:        1438
  Meter Flags:            KBPS BURST STATS
  Flow Count:            0
  Number of  bands:      2
  In packet count:       -NA-
  In byte count:         0

  Band Type:    DSCP-REMARK

    Rate:                          750000
    Burst size:                    1500          kb
    Prec level:                    1
    In packet band count:          -NA-
    In byte band count:            0


  Band Type:    DROP

    Rate:                          1000000
    Burst size:                    2000          kb
    In packet band count:          -NA-
    In byte band count:            0

----
Total no. of entries printed: 1
```

The following example displays output with specific meter in LP.

```
device(config)# show openflow meters 1
Meter id: 1023

  Meter Flags:                    KBPS BURST
  Number of  bands:              2
  RL Class Index:                33      33
  In packet count:               -NA-
  In byte count:                 0

  Band Type:    DROP

    Rate:                          3000         Adjusted rate:2996
    Burst size:                    1250          kb
    In packet band count:          -NA-
    In byte band count:            0

Band Type:    DSCP-REMARK

    Rate:                          1700         Adjusted rate:1693
    Burst size:                    1250          kb
    Prec level:                    27
    In packet band count:          -NA-
    In byte band count:            0
```

History

Release version	Command history
5.7.00	This command was introduced.

show openflow queues

Displays the queues on the OpenFlow ports.

Syntax

show openflow queues [**ethernet** *slot* **/** *port*]

show openflow queues [**ethernet** *slot* **/** *port* **to** *slot* **/** *port*]

Parameters

ethernet *slot* **/** *port*

Gives information about a particular slot and port in an ethernet.

to

Indicates a range of ports.

Modes

User EXEC mode

Usage Guidelines

You can specify additional ports with additional **ethernet** *slot* **/** *port* elements.

You can specify additional ports ranges with additional **ethernet** *slot* **/** *port* **to** *slot* **/** *port* elements.

Command Output

The **show openflow queues** command displays the following information:

Output field	Description
Queue	Number of queues
Rate	Minimum and maximum rate of the queue
Packet	Number of packet in the queue
Bytes	Number of bytes in the queue

Examples

The following example displays openflow queues on a specified port.

```
device#show openflow queues ethernet 2/1

Openflow Port    2/1
  Queue 0
   Min Rate: 0           Max Rate: 0
   Tx Packets: 0
   Tx Bytes: 0
Openflow Port    2/1
  Queue 1
   Min Rate: 0           Max Rate: 0
   Tx Packets: 0
   Tx Bytes: 0
Openflow Port    2/1
  Queue 2
   Min Rate: 0           Max Rate: 0
   Tx Packets: 0
   Tx Bytes: 0
Openflow Port    2/1
  Queue 3
   Min Rate: 0           Max Rate: 0
   Tx Packets: 0
   Tx Bytes: 0
Openflow Port    2/1
  Queue 4
   Min Rate: 0           Max Rate: 0
   Tx Packets: 1918620
   Tx Bytes: 168838560
Openflow Port    2/1
  Queue 5
   Min Rate: 0           Max Rate: 0
   Tx Packets: 0
   Tx Bytes: 0
Openflow Port    2/1
  Queue 6
   Min Rate: 0           Max Rate: 0
   Tx Packets: 0
   Tx Bytes: 0
Openflow Port    2/1
  Queue 7
   Min Rate: 0           Max Rate: 0
   Tx Packets: 0
   Tx Bytes: 0
```

History

Release version	Command history
5.7.00	This command was introduced.

show packet-encap-processing

Use the **show packet-encap-processing** command to view the configured packet encapsulation processing.

Syntax

show packet-encap-processing

Modes

EXEC mode and configuration (config) mode.

Examples

An example output of the **show packet-encap-processing** command.

```
device # show packet-encap-processing

 ON      : Feature is configured
 -       : Feature is not configured
 *       : Feature is not supported
 <Blank> : Slot is Empty
-------------------------------------------------------------------
| Slot| Dev| 802.1BR| 802.1BR| VN-Tag | VN-Tag | NVGRE  | VXLAN   |
| Id  | Id | Strip  | Bypass | Strip  | Bypass | Strip  | Strip   |
-------------------------------------------------------------------
| S1  | 1  | -      | -      | -      | -      | ON     |  ON     |
|     | 2  | -      | -      | -      | -      | ON     |  ON     |
-------------------------------------------------------------------
| S2  | 1  | -      | -      | -      | -      | ON     |  ON     |
|     | 2  | -      | -      | -      | -      | ON     |  ON     |
-------------------------------------------------------------------
| S3  | 1  | -      | -      | -      | -      | ON     |  ON     |
|     | 2  | -      | -      | -      | -      | ON     |  ON     |
-------------------------------------------------------------------
| S4  | 1  | -      | -      | -      | -      | ON     |  ON     |
|     | 2  | -      | -      | -      | -      | ON     |  ON     |
-------------------------------------------------------------------
```

History

Release version	Command history
6.0.00a	This command was introduced.
6.1.0	This command was modified to display VXLAN strip configuration.

show packet-encap-processing slot

Displays the packet encapsulation processing configuration on the selected slot.

Syntax

show packet-encap-processing { **slot** *slot-num* }

Parameters

slot

Slot number

Modes

EXEC mode

Examples

An example of show packet encapsulation processing configuration on slot 1.

```
device(config)# show packet-encap-processing slot 1
ON      : Feature is configured
 -       : Feature is not configured
 *       : Feature is not supported
 <Blank> : Slot is Empty
-----------------------------------------------------------
| Slot| Dev| 802.1BR| 802.1BR| VN-Tag | VN-Tag | NVGRE  |
| Id  | Id | Strip  | Bypass | Strip  | Bypass | Strip  |
-----------------------------------------------------------
| S1  | 1  | -      | ON     | -      | -      | -      |
|     | 2  | -      | -      | ON     | -      | -      |
-----------------------------------------------------------
```

History

Release version	Command history
6.0.00a	This command was introduced.

show packet-encap-processing strip-802-1BR

Displays the packet encapsulation processing when strip-802-1BR has been configured.

Syntax

show packet-encap-processing strip-802-1BR

Modes

EXEC mode.

Examples

An example output of the **show packet-encap-processing strip-802-1BR** command.

```
device(config)# show packet-encap-processing strip-802-1BR
ON      : Feature is configured
 -       : Feature is not configured
 *       : Feature is not supported
 <Blank> : Slot is Empty
----------------------------
| Slot| Dev| 802.1BR Strip |
----------------------------
| S1  | 1  | -             |
|     | 2  | -             |
----------------------------
| S2  | 1  | *             |
|     | 2  | *             |
----------------------------
| S3  | 1  | *             |
|     | 2  | *             |
----------------------------
| S4  | 1  | -             |
|     | 2  | ON            |
----------------------------
```

History

Release version	Command history
6.0.00a	This command was introduced.

show packet-encap-processing strip-vn-tag

Displays the packet encapsulation processing when strip-vn-tag has been configured.

Syntax

show packet-encap-processing strip-vn-tag

Modes

EXEC mode.

Examples

An example output of the **show packet-encap-processing strip-vn-tag** command.

```
device(config)# show packet-encap-processing strip-vn-tag
ON      : Feature is configured
 -       : Feature is not configured
 *       : Feature is not supported
 <Blank> : Slot is Empty
----------------------------
| Slot| Dev| VN-Tag Strip  |
----------------------------
| S1  | 1  | -             |
|     | 2  | ON            |
----------------------------
| S2  | 1  | *             |
|     | 2  | *             |
----------------------------
| S3  | 1  | *             |
|     | 2  | *             |
----------------------------
| S4  | 1  | -             |
|     | 2  | -             |
----------------------------
```

History

Release version	Command history
6.0.00a	This command was introduced.

show packet-encap-processing interface ethernet

Displays the packet encapsulation processing configuration on the selected interface ethernet.

Syntax

show packet-encap-processing interface ethernet { **slot** *slot-num* **port** *port-num* }

Parameters

slot

Slot number

port

Port number.

Modes

EXEC mode

Examples

An example of packet encapsulation processing configuration on interface ethernet 1/1.

```
device(config)# show packet-encap-processing interface ethernet 1/1
------------------------------------------------------------
  Port State :                  Disabled
------------------------------------------------------------
  Feature-Name                  Status
  802.1BR Stripping             ON
  802.1BR Preservation          OFF
  VN-tag Stripping              OFF
  VN-tag Preservation           OFF
  NVGRE Stripping               OFF
------------------------------------------------------------
```

History

Release version	Command history
6.0.00a	This command was introduced.

show pim interface

Displays the IPv4 or IPv6 PIM interface table.

Syntax

show { **ip** | **ipv6** } **pim interface**

Parameters

ip

Displays the IPv4 PIM interface table.

ipv6

Displays the IPv6 PIM interface table.

Modes

User EXEC mode

Examples

The following is a sample display of the **show ip pim interface** command.

```
device# show ip pim interface

---------+--------+---+---+------------+---+---------+-------+----+----+--------+
Interface|Local   |Ver|St |Router      |TTL|Multicast| Filter|VRF | DR |Override
         |Address |   |   |Address Port|Thr|Boundary | ACL   |    |Prio|Interval
---------+--------+---+---+------------+---+---------+-------+----+----+--------+
e1/3      3.3.3.1 DMv2 Ena Itself       1   None       10   default 1   3000ms
e1/2      2.2.2.1 DMv2 Ena 2.2.2.2 1/2  1   None       None default 1   3000ms
Total Number of Interfaces: 2
```

History

Release	Command History
5.5.00	This command was modified to display neighbor routers on an interface.

show pim multicast-filter

Displays the multicast filters on a interface or globally for the hardware.

Syntax

show { **ip** | **ipv6** } **pim**

Modes

User EXEC mode

Examples

Show output for global.

```
device# show ip pim vrf multicast-filter
-------------------------------------------------------------------------------
Interface|LAG Member  |port |vlan  | Multicast Filter |CAM Index| ProgTM
-------------------------------------------------------------------------------
    *           -               *         *     1.1.1.1, 239.1.1.1    0x343    22:01:33
    *           -               *         *           *,     234.1.1.1        0x344    22:01:33
```

Show output for interface .

```
device# show ip pim interface
-------------------------------------------------------------------------------
Interface    |LAG Member    |port    |vlan    |Multicast Filter        |CAM Index|ProgTM
-------------------------------------------------------------------------------
ve100        -        *         100     1.1.1.1, 239.1.1.1    0x343    22:01:33
ve102        -        *         100           *,     234.1.1.1    0x344    22:01:33
e1/13        -        142    100            *, 228/8        0x355    22:01:33
Tr1(e1/1)        e1/1        155    1             *, 228/8        0x356    22:01:33
            e1/4        156    1             *, 228/8        0x357    22:01:33
Tn1             -        *    *        *, 228/8        0x358    22:01:33
```

History

Release version	Command history
NI05.7.00	This command was introduced.

show pki certificates

Displays certificate information associated with a trustpoint or the local router.

Syntax

show pki certificates trustpoint *trustpoint-name* [**detail**]

show pki certificates local [**detail**]

Parameters

trustpoint *trustpoint-name*

Displays certificate information associated with a trustpoint certificate authority (CA).

detail

Displays detailed information about the certificate.

local

Displays certificate information associated with a local certificate provided for the device.

detail

Displays detailed information about the certificate.

Modes

User EXEC mode

Examples

The following example displays output for the trustpoint with the name "brocade".

```
device# show pki certificates trustpoint brocade

----------------PKI TRUSTPOINT CERTIFICATE ENTRY-----------------
Certificate:
    Data:
        Version: 3 (0x00000002)
        Serial Number:
            fe:75:d1:a3:bc:56:28:8e
    Signature Algorithm: ecdsa-with-SHA1
        Issuer: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
emailAddress=brocade_ca@brocade.com
        Validity
            Not Before: Aug 29 05:58:13 2014 GMT
            Not After : Aug 29 05:58:13 2019 GMT
        Subject: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
emailAddress=brocade_ca@brocade.com
```

The following example displays the detailed output for the trustpoint with the name "brocade".

```
device# show pki certificates trustpoint brocade detail

----------------PKI TRUSTPOINT CERTIFICATE ENTRY-----------------
Certificate:
    Data:
        Version: 3 (0x00000002)
        Serial Number:
            fe:75:d1:a3:bc:56:28:8e
    Signature Algorithm: ecdsa-with-SHA1
        Issuer: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
emailAddress=brocade_ca@brocade.com
        Validity
            Not Before: Aug 29 05:58:13 2014 GMT
            Not After : Aug 29 05:58:13 2019 GMT
        Subject: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
emailAddress=brocade_ca@brocade.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:bf:02:57:b0:9e:db:5d:c6:f3:e0:1a:09:c1:ca:
                    0f:8b:ed:c0:14:3d:41:ec:d0:a3:98:85:2a:4b:0e:
                    74:36:04:c3:c9:51:e6:dd:b6:19:d6:8b:38:99:9a:
                    b7:27:89:4b:5f:cf:fe:15:1a:f1:c4:61:ce:b7:c6:
                    70:47:4c:4c:b4:57:e6:57:37:71:46:98:84:95:0a:
                    47:60:42:35:7b:d3:a1:a7:78:5f:92:68:d0:5a:f8:
                    b8:7e:5f:83:01:14:16
                ASN1 OID: secp384r1
            X509v3 extensions:
                X509v3 Subject Key Identifier:
                    63:30:96:B1:59:36:FB:B4:07:44:47:28:D6:35:34:5A:80:55:AB:FD
                X509v3 Authority Key Identifier:
                    keyid:63:30:96:B1:59:36:FB:B4:07:44:47:28:D6:35:34:5A:80:55:AB:FD


X509v3 Basic Constraints:
X509                CA:TRUE
    Signature Algorithm: ecdsa-with-SHA1
         30:64:02:30:1e:00:81:91:59:c1:ba:5f:ce:fe:c9:ca:98:e7:
         b2:98:3b:f5:e9:7b:35:ea:2e:c6:b1:ba:77:14:ef:d0:46:ff:
         30:cb:da:a7:64:65:f0:18:80:95:b0:a5:f7:f4:c4:28:02:30:
         2a:0a:4f:1f:19:a9:a3:67:99:3e:05:bb:74:ac:b8:2f:e2:75:
         5d:90:b5:18:74:ae:5c:7a:e8:27:93:c4:e2:34:3e:34:9b:4a:
         17:ea:3a:2e:7e:90:a8:1d:ea:45:bd:12
```

The following example displays the output for the local certificate.

```
device# show pki certificates local

----------------PKI LOCAL CERTIFICATE ENTRY-----------------
Certificate:
    Data:
        Version: 3 (0x00000002)
        Serial Number: 1 (0x00000001)
    Signature Algorithm: ecdsa-with-SHA1
        Issuer: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_RA/
emailAddress=brocade_ra@brocade.com
        Validity
            Not Before: Sep 10 14:55:12 2014 GMT
            Not After : Jun  1 14:55:12 2016 GMT
        Subject: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_mlx1/
emailAddress=Brocade_mlx1@brocade.com
```

History

Release version	Command history
5.8.00	This command was introduced.

show pki counters

Displays the Public Key Infrastructure (PKI) counter information for a certificate authority (CA).

Syntax

show pki counters

Modes

User EXEC mode

Examples

The following example displays information about the PKI counter information for a CA.

```
device# show  pki counters
 PKI Sessions Started: 5
 PKI Sessions Ended: 5
 PKI Sessions Active: 0
 Successful Validations: 1
 Failed Validations: 4
 Bypassed Validations: 0
 Pending Validations: 0
 CRLs checked: 3
 CRL - fetch attempts: 2
 CRL - failed attempts: 0
```

History

Release version	Command history
5.9.00	This command was introduced.

show pki crls

Displays the Public Key Infrastructure (PKI) Certification Revocation list (CRL).

Syntax

show pki crls *trustpoint name*

Parameters

trustpoint name

The specific trustpoint name whose PKI CRLs need to be displayed.

Modes

User EXEC mode

Examples

The following example displays the PKI CRL list.

```
device# show  pki crls
 CRL Issuer Name:
 cn=name Cert Manager,ou=pki,o=company.com,c=US
 CRL number: 24
 CRL Version: V2
 LastUpdate: 18:57:42 GMT March 4 2013
 NextUpdate: 22:57:42 GMT March 4 2013
 Retrieved from CRL Distribution Point:
  via SCEP
```

History

Release version	Command history
5.9.00	This command was introduced.

show pki enrollment-profile

Displays the Public Key Infrastructure (PKI) enrollment profile details.

Syntax

show pki enrollment-profile *profile name*

Parameters

profile name

Specifies the PKI enrollment profile name.

Modes

User EXEC mode

Examples

The following example displays information about the PKI enrollment profiles.

```
device# show pki enrollment-profile

----------------PKI ENROLLMENT PROFILE ENTRY-----------------
  Enrollment Profile: John
  Authentication Command: win-hj98ak136a0.englab.brocade.com_englab-WIN-N6C3R0LUDAJ-CA-7
  Authentication URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
  Enrollment URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
  SCEP password: 8A4976CE110A8686


----------------PKI ENROLLMENT PROFILE ENTRY-----------------
  Enrollment Profile: Jane


----------------PKI ENROLLMENT PROFILE ENTRY-----------------
  Enrollment Profile: John
  Authentication Command: win-hj98ak136a0.englab.brocade.com_englab-WIN-N6C3R0LUDAJ-CA-7
  Authentication URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
  Enrollment URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
  SCEP password: 8A4976CE110A8686
```

History

Release version	Command history
5.9.00	This command was introduced.

show pki entity

Displays the PKI entity details.

Syntax

show pki entity *entity-name*

Parameters

entity-name

The entity name.

Modes

User EXEC mode

Examples

The following example displays the output for the entity name "brocade_entity".

```
device# show pki entity brocade_entity

----------------PKI ENTITY ENTRY-----------------
  Entity Name: brocade_entity
  Common Name: brocade_e
  Organization Name: Brocade
  Organization Unit Name: Routing
  State Name: Karnataka
  Country Name: India
  Email: user@brocade.com
  FQDN: brocade-fqdn
  Subject Alternative Name: brocade-subject
  Location: Bangalore
  IP Address: 1.1.1.1
```

History

Release version	Command history
5.8.00	This command was introduced.

show pki key mypubkey

Displays the PKI public keys on the NetIron device.

Syntax

show pki key mypubkey ec manual [**label** *label-string*]

Parameters

ec

The manually configured Elliptic Curve (EC) key.

manual

The manually configured key.

label

The ID given to the key.

label-string

The name of the label.

Modes

User EXEC mode

Examples

The following example displays the output for the manually generated PKI keys.

```
device# show pki key mypubkey ec manual label xmr-key

----------------PKI PUBLIC KEY ENTRY-----------------
 Public key of manual EC key pair:
  The key label is xmr-key
  Public-Key: (384 bit)
  pub:
      04:33:a6:3e:8e:94:ab:49:b8:e4:dd:f1:f9:2d:78:
      28:65:81:43:08:bd:b7:90:e8:90:56:4d:2e:7b:44:
      51:bf:bc:59:78:87:27:51:5c:b6:c0:75:d5:51:28:
      3b:37:3f:71:62:8e:20:98:b5:fe:72:69:ab:a2:69:
      22:eb:de:27:58:d6:00:66:f0:cc:7f:d2:30:4c:c1:
      a8:f8:d2:c9:6b:39:76:1a:66:f0:82:f2:2e:44:e5:
      3e:56:a3:f3:5b:76:81
  ASN1 OID: secp384r1
```

History

Release version	Command history
5.8.00	This command was introduced.

show pki trustpoint

Displays a PKI Certificate Authority (CA) status and its certificate.

Syntax

show pki trustpoint *trustpoint-name* [**status**]

Parameters

trustpoint-name

The name of the CA.

status

The status of the PKI certificate.

Modes

User EXEC mode

Examples

The following example displays the output for a CA that is not authenticated.

```
device# show pki trustpoint status
! CA is not authenticated, and is queried
 CA Test, VRF: Default
 Issuing CA certificate status: pending
 Subject Name:
 cn=r1 Cert Manager,ou=pki,o=company.com,c=country
 Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
 Router certificate status: pending
 Subject Name:
 hostname=host.company.com,o=company.com
 Next query attempt: 52 seconds
```

The following example displays the output for a CA that is authenticated but the request has not started.

```
device# show pki trustpoint status
! CA is authenticated, and certificate request is not started
 CA Test, VRF: Default
 Issuing CA certificate: configured
 Subject Name:
 cn=r1 Cert Manager,ou=pki,o=company.com,c=country
 Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
 State:
 Keys Generated | CA Authenticated | Certificate Request
 No             | Yes              | None
```

The following example displays the output for a CA that is authenticated but the certificate request is pending.

```
device# show pki trustpoint status
 ! CA is authenticated, and certificate request is pending
 CA Test, VRF: Default
 Issuing CA certificate: configured
 Subject Name:
 cn=r1 Cert Manager,ou=pki,o=company.com,c=country
 Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
 Router Signature certificate pending:
 Requested Subject Name:
 hostname=host.company.com
 Request Fingerprint: FAE0D74E BB844EA1 54B26698 56AB42EC
 Enrollment polling: 1 times (9 left)
 Next poll: 32 seconds
 Last enrollment status: Pending
 State:
 Keys Generated | CA Authenticated | Certificate Request
 yes(signature) | Yes              | Pending
```

The following example displays the output for a CA that is authenticated and the certificate is granted.

```
device# show pki trustpoint status
! CA is authenticated, and certificate is granted
 CA Test, VRF: Default
 Issuing CA certificate: configured
 Subject Name:
 cn=r1 Cert Manager,ou=pki,o=company.com,c=country
 Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
 Router Signature certificate configured:
 Subject Name:
 hostname=host.company.com,o=company.com
 Fingerprint: 8A370B8B 3B6A2464 F962178E 8385E9D6
 Router Encryption certificate configured:
 Subject Name:
 hostname=host.company.com,o=company.com
 Fingerprint: 43A03218 C0AFF844 AE0C162A 690B414A
 Last enrollment status: Granted
 State:
 Keys Generated | CA Authenticated | Certificate Request
 yes(signature) | Yes              | yes
```

The following example displays the output for a CA trustpoint.

```
device# show pki trustpoint
 CA test, VRF: Default
 Subject Name:
 cn=Brocade
 o=Company
 Serial Number: 0FFEBBDC1B6F6D9D0EA7875875E4C695
 Certificate configured.
 Enrollment Protocol:
 SCEP, Regenerate at 80%
```

History

Release version	Command history
5.8.00	This command was introduced.

show rate-limit counters bum-drop

Displays the per-port / per-VLAN rate-limiting information for broadcast/unicast/multicast (BUM) traffic.

Syntax

show rate-limit counters bum-drop

show rate-limit counters bum-dropport-id *slot* **/** *port* [**all** | **vlan** *vlan-id*]

Parameters

port-id *slot* **/** *port*

Displays the information for a specified port.

all

Displays the information for all BUM counters on the specified port.

vlan *vlan-id*

Displays the information for all BUM counters on the specified VLAN.

Modes

User EXEC mode

Command Output

The **show rate-limit counters bum-drop** command displays the following information:

Output field	Description
interface	Displays the interface information for which the rate-limiting accounting is configured.
port: Drop:	Displays information about the BUM traffic (in bytes) that has been dropped as a result of the defined rate limit policy for the specific port defined.
rate-limit input broadcast	Displays information about the BUM traffic (in bytes) that has been dropped as a result of the defined rate limit policy.
vlan-id: 100 Drop	Displays information about the BUM traffic (in bytes) that has been dropped as a result of the defined rate limit policy for the specific VLAN id defined.

Examples

The following example for **show rate-limit counters bum-drop** command displays the following information.

```
Brocade(config-if-e10000-5/1)#sh rate-limit counters bum-drop

interface e 5/1
rate-limit input broadcast 993568 10000
port: Drop: 0 bytes
rate-limit input vlan-id 100 broadcast 993568 100000
vlan-id: 100 Drop: 0 bytes

Brocade(config-if-e10000-5/1)#sh rate-limit counters bum-drop port-id 5/1

interface e 5/1
rate-limit input broadcast 993568 10000
port: Drop: 0 bytes

Brocade(config-if-e10000-5/1)#sh rate-limit counters bum-drop port-id 5/1 vlan-id 100

interface e 5/1
rate-limit input vlan-id 100 broadcast 993568 100000
vlan-id: 100 Drop: 0 bytes
```

History

Release version	Command history
5.7.00	This command was introduced.

show rate-limit detail

Displays detailed information for all interfaces, including the per-port / per-VLAN rate-limiting information.

Syntax

show rate-limit detail

Modes

User EXEC mode.

Examples

The **show rate-limit detail** command displays the following information.

```
Brocade#show rate-limit detail
interface e 8/1
rate-limit input vlan-id 2 broadcast multicast 97728 10000 include-  control
rate-limit input broadcast multicast 97728 10000 include-control
rate-limit input access-group name ipv4_acl 100000 10000 include-control
rate-limit input access-group name ipv6_acl 100000 10000 include-control
rate-limit input access-group name ipv6_acl policy ipv6_map include-control
```

History

Release version	Command history
5.7.00	This command was introduced.

show rate-limit interface

Displays the rate-limiting information for the interface indicated.

Syntax

show rate-limit interface [*slot/port*]

Modes

User EXEC mode.

Examples

The **show rate-limit interface** command displays the following information.

```
Brocade#show rate-limit interface
interface e 8/1
rate-limit input vlan-id 2 broadcast multicast 97728 10000 include-  control
rate-limit input broadcast multicast 97728 10000 include-control
rate-limit input access-group name ipv4_acl 100000 10000 include-control
```

History

Release version	Command history
5.7.00	This command was introduced.

show rate-limit ipv6 hoplimit-expired-to-cpu

Displays the information about rate-limit configuration on IPv6 hoplimit-not-ok packets.

Syntax

show rate-limit ipv6 hoplimit-expired-to-cpu

Modes

User EXEC mode

Command Output

The **show rate-limit ipv6 hoplimit-expired-to-cpu** command displays the following information:

Output field	Description
Fwd	The hoplimit-expired-to-cpu traffic in bytes that has been sent to the CPU as a result of the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.
Drop	The hoplimit-expired-to-cpu traffic in bytes that has been dropped as a result of the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.
Re-mark	The hoplimit-expired-to-cpu traffic in bytes whose priority have been remarked as a result of exceed the bandwidth available in the CIR bucket for the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.
Total	The total hoplimit-expired-to-cpu traffic in bytes that has been subjected to the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.

Examples

This example displays output of the **show rate-limit ipv6 hoplimit-expired-to-cpu** command.

```
device#show rate-limit ipv6 hoplimit-expired-to-cpu
Fwd: 1865392 Drop: 867731400 bytes
Re-mark: 1864800 Total: 871461592 bytes
```

History

Release version	Command history
5.8.00	This command was introduced.

show rate-limit option-pkt-to-cpu

Displays the information about rate-limit configuration on IPv4 option packets.

Syntax

show rate-limit option-pkt-to-cpu

Modes

User EXEC mode

Command Output

The **show rate-limit option-pkt-to-cpu** command displays the following information:

Output field	Description
Fwd	The IPv4 option-pkt-to-cpu traffic in bytes that has been sent to the CPU as a result of the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.
Drop	The IPv4 option-pkt-to-cpu traffic in bytes that has been dropped as a result of the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.
Re-mark	The IPv4 option-pkt-to-cpu traffic in bytes whose priority have been remarked as a result of exceed the bandwidth available in the CIR bucket for the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.
Total	The total IPv4 option-pkt-to-cpu traffic in bytes that has been subjected to the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.

Examples

This example displays of the **show rate-limit option-pkt-to-cpu** command.

```
device# show rate-limit option-pkt-to-cpu
Fwd: 1865392 Drop: 867731400 bytes
Re-mark: 1864800 Total: 871461592 bytes
```

History

Release version	Command history
5.8.00	This command was introduced.

show rate-limit ttl-expired-to-cpu

Displays the information about rate-limit configuration on IPv4 ttl-expired-to-cpu packets.

Syntax

show rate-limit ttl-expired-to-cpu

Modes

User EXEC mode

Command Output

The **show rate-limit ttl-expired-to-cpu** command displays the following information:

Output field	Description
Fwd	The ttl-expired-to-cpu traffic in bytes that has been sent to the CPU as a result of the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.
Drop	The ttl-expired-to-cpu traffic in bytes that has been dropped as a result of the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.
Re-mark	The ttl-expired-to-cpu traffic in bytes whose priority have been remarked as a result of exceed the bandwidth available in the CIR bucket for the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.
Total	The total ttl-expired-to-cpu traffic in bytes that has been subjected to the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.

Examples

This example displays output of the **show rate-limit ttl-expired-to-cpu** command.

```
device# show rate-limit ttl-expired-to-cpu
Fwd: 1865392 Drop: 867731400 bytes
Re-mark: 1864800 Total: 871461592 bytes
```

History

Release version	Command history
5.8.00	This command was introduced.

show rmon alarm

Displays the Remote monitoring (RMON) alarm events.

Syntax

show rmon alarm [*number*]

Parameters

number

Specifies a RMON alarm number.

Modes

User EXEC mode

Usage Guidelines

An RMON alarm is designed to monitor configured thresholds. An alarm event is reported each time that a threshold is exceeded. The alarm entry also indicates the action (event) to be taken if the threshold be exceeded.

show rmon statistics

Displays the Remote monitoring (RMON) agent status and information about RMON statistics.

Syntax

show rmon statistics [*number* | **ethernet** *slot*/*port* | **management** *port*]

Parameters

number

Displays the RMON statistics for a specific statistics index identification number. Valid values range from 1 through 65535.

ethernet *slot port*

Displays the RMON statistics for a specific Ethernet interface.

management *port*

Displays the RMON statistics for a specific management port.

Modes

User EXEC mode

Usage Guidelines

Entering the **show rmon statistics** command without any options displays statistics for all ports.

Command Output

The **show rmon statistics** command displays the following information:

Output field	Description
Octets	The total number of octets of data received on the network. This number includes octets in bad packets. This number does not include framing bits but does include Frame Check Sequence (FCS) octets.
Drop events	Indicates an overrun at the port. The port logic could not receive the traffic at full line rate and had to drop some packets as a result. The counter indicates the total number of events in which packets were dropped by the RMON probe due to lack of resources. This number is not necessarily the number of packets dropped, but is the number of times an overrun condition has been detected.
Packets	The total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.
Broadcast pkts	The total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Multicast pkts	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC align errors	The total number of packets received that were from 64 - 1518 octets long, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral

Output field	Description
	number of octets (Alignment Error). The packet length does not include framing bits but does include FCS octets.
Undersize pkts	The total number of packets received that were less than 64 octets long and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Fragments	The total number of packets received that were less than 64 octets long and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for this counter to increment, since it counts both runts (which are normal occurrences due to collisions) and noise hits. This number does not include framing bits but does include FCS octets.
Oversize packets	The total number of packets received that were longer than 1518 octets and were otherwise well formed. This number does not include framing bits but does include FCS octets. 48GC modules do not support count information on oversized packets and report 0.
Jabbers	The total number of packets received that were longer than 1518 octets and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). This number does not include framing bits but does include FCS octets. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 octets pkts	The total number of packets received that were 64 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
65 to 127 octets pkts	The total number of packets received that were 65 - 127 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
128 to 255 octets pkts	The total number of packets received that were 128 - 255 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
256 to 511 octets pkts	The total number of packets received that were 256 - 511 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
512 to 1023 octets pkts	The total number of packets received that were 512 - 1023 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
1024 to Max size	The total number of packets received that were 1024 octets - the maximum size of octets. This number includes bad packets. This number does not include framing bits but does include FCS octets.

Examples

The following example displays statistics for all RMON ports.

```
device(config)# show rmon statistics
Ethernet statistics 1 is active, owned by monitor
 Interface 1/1 (ifIndex 1) counters
                  Octets          0
             Drop events          0                    Packets          0
          Broadcast pkts          0            Multicast pkts          0
    CRC alignment errors          0            Undersize pkts          0
           Oversize pkts          0                 Fragments          0
                 Jabbers          0                Collisions          0
          64 octets pkts          0     65 to 127 octets pkts          0
  128 to 255 octets pkts          0    256 to 511 octets pkts          0
  512 to 1023 octets pkts         0  1024 to 1518 octets pkts          0
```

show route-map

Displays route map information.

Syntax

show route-map *name*| **binding**

Parameters

map-name

Shows details of the matched UDA ACL configured in the route map, along with the IPv4 ACL and IPv6 ACL.

binding

Shows the UDA PBR binding along with IPv4 and IPv6 PBR bindings. This command is supported in the LP only.

Modes

EXEC mode

Examples

The following example below shows the output of the command.

```
device(config)# show route-map
route-map Test1 permit 1
 match uda  udaAcl
 match ip address  101
 set next-hop-flood-vlan 10
```

The following example show the command using the **binding** option.

```
device# show route-map  binding
IPv4 Bindings of Test1 :
  4/4
UDA PBR Bindings of Test2 :
  3/1
```

History

Release version	Command history
5.9.00	This command was modified to support UDA PBR information.

show rstp

Displays Rapid Spanning Tree Protocol (RSTP) information.

Syntax

show rstp [**blocked**] [**vlan vlan-id**]

Parameters

blocked

Displays information in respect of ports blocked by the RSTP only.

vlan *vlan-id*

Displays RSTP information for a specific VLAN.

Modes

User EXEC mode

Usage Guidelines

This command can also be entered in global configuration mode.

Examples

The following example displays a summary of RSTP information for VLAN 10:

```
device> show rstp vlan 10

VLAN 10 - RSTP instance 0
------------------------------------------------------------------
RSTP (IEEE 802.1w) Bridge Parameters:
Bridge           Bridge Bridge Bridge Force    tx
Identifier       MaxAge Hello  FwdDly Version  Hold
hex              sec    sec    sec             cnt
0001000480a04000 20     2      15     Default  3
RootBridge       RootPath  DesignatedBridge Root  Max Hel Fwd
Identifier       Cost      Identifier       Port  Age lo  Dly
hex                        hex                    sec sec sec
0001000480a04000 0         0001000480a04000 Root  20  2   15
RSTP (IEEE 802.1w) Port Parameters:
      <--- Config Params -->|<-------------- Current state ----------------->
Port  Pri PortPath  P2P Edge Role       State      Designa-  Designated
Num       Cost      Mac Port                      ted cost  bridge
1/3   128 20000     T   F    DISABLED   DISABLED   0         0000000000000000
1/13  128 20000     T   F    DISABLED   DISABLED   0         0000000000000000
```

The following example displays a summary of ports blocked by RSTP on VLAN 20:

```
device> show rstp blocked vlan 20

VLAN 20 - RSTP instance 0
------------------------------------------------------------------------
RSTP (IEEE 802.1w) Bridge Parameters:

Bridge           Bridge Bridge Bridge Force    tx
Identifier       MaxAge Hello  FwdDly Version  Hold
hex              sec    sec    sec             cnt
80000024389e2d20 20     2      15     Default  3

RootBridge       RootPath  DesignatedBridge Root  Max Hel Fwd
Identifier       Cost      Identifier       Port  Age lo  Dly
hex                        hex                    sec sec sec
80000024388f6b20 2000      80000024388f6b20 3/5   20  2   15

RSTP (IEEE 802.1w) Port Parameters:

      <--- Config Params -->|<-------------- Current state ----------------->
Port  Pri PortPath  P2P Edge Role       State      Designa-  Designated
Num       Cost      Mac Port                      ted cost  bridge
3/6   128 2000      F   F    ALTERNATE  DISCARDING 0         80000024388f6b20
3/7   128 2000      F   F    ALTERNATE  DISCARDING 0         80000024388f6b20
3/8   128 2000      F   F    ALTERNATE  DISCARDING 0         80000024388f6b20
```

History

Release	Command History
5.5.00	The command was modified to display only ports blocked by the RSTP.

show running-config

Displays the current running configuration.

Syntax

show running-config

Parameters

interface

Displays the running-configuration section.

ethernet *slot/port*

Displays the specified ethernet port.

loopback *num*

Displays the loopback port.

pos *slot/port*

Displays the specified POS port.

tunnel *num*

Displays the specified tunnel port.

ve *num*

Displays the specified Virtual Ethernet (VE) port.

lag

Displays the LAG running-configuration section.

detailed

Displays the LAG running-configuration information in detail.

id *lag_id*

Displays the specified LAG running-configuration.

name *lag_name*

Displays the specified LAG running-configuration name.

vlan

Displays the VLAN running-configuration section.

Modes

User EXEC mode

Usage Guidelines

Use this command with filtering for the specific command for which you want to review the current configuration on the device. Most commands are available in this format using either the begin or the include options. See the Example section for examples of each option.

Examples

The following example displays the **show running-config** command. Notice that the interface bandwidth command is displayed as part of the interface configuration.

```
device#show running-config interface tunnel 2
interface tunnel 2
 tunnel mode gre ip
 tunnel source 169.70.15.2
 tunnel destination 169.70.15.1
 ip address 199.0.0.2/24
 bandwidth 2000
```

The following example displays the **show running-config** command executed on an Ethernet interface.

```
device#show running-config interface ethernet 8/1
interface e 8/1
rate-limit input vlan-id 2 broadcast multicast 97728 10000 include-  control
rate-limit input broadcast multicast 97728 10000 include-control
rate-limit input access-group name ipv4_acl 100000 10000 include-control
```

History

Release version	Command history
5.7.00	This command was modified to include the interface bandwidth command as part of the interface configuration.

show sflow statistics

Displays the total count per interface for both sFlow and ACL-based samples in all slots where sFlow is configured.

Syntax

show sflow statistics *slot*/*port*

Parameters

slot port Displays statistics for the specified port.

Modes

User EXEC mode

Usage Guidelines

History

Release	Command History
5.5.00	This command was modified to display sFlow statistics information.

show spanning-tree

Displays Spanning Tree Protocol (STP) information.

Syntax

show spanning-tree [**blocked**] [**vlan** *vlan-id* [**ethernet** *slot*/*port*]]

Parameters

blocked

Displays information for ports blocked by the STP only.

vlan *vlan-id*

Displays information for a specific port-based VLAN.

ethernet *slot port*

Displays information for a specific Ethernet interface on a port-based VLAN.

Modes

User EXEC mode

Usage Guidelines

This command is also available in global configuration mode.

Examples

The following example displays STP information for VLAN 10:

```
device> show spanning-tree vlan 10

VLAN 10 - STP instance 1
------------------------------------------------------------------
STP Bridge Parameters:
Bridge           Bridge Bridge Bridge Hold  LastTopology Topology
Identifier       MaxAge Hello  FwdDly Time  Change       Change
hex              sec    sec    sec    sec   sec          cnt
8000000480a04000 20     2      15     1     0            0
RootBridge       RootPath  DesignatedBridge Root  Max Hel Fwd
Identifier       Cost      Identifier       Port  Age lo  Dly
hex                        hex                    sec sec sec
8000000480a04000 0         8000000480a04000 Root  20  2   15
STP Port Parameters:
Port  Prio Path      State      Designat- Designated       Designated
Num   rity Cost                ed Cost   Root             Bridge
1/3   128  4         DISABLED   0         0000000000000000 0000000000000000
1/13  128  4         DISABLED   0         0000000000000000 0000000000000000
```

The following example displays STP information for VLAN 10, listing blocked ports only:

```
device> show spanning-tree blocked vlan 10

VLAN 10 - STP instance 0
------------------------------------------------------------------------
STP Bridge Parameters:
Bridge           Bridge Bridge Bridge Hold  LastTopology Topology
Identifier       MaxAge Hello  FwdDly Time  Change       Change
hex              sec    sec    sec    sec   sec          cnt
80000024389e2d00 20     2      15     1     718          1
RootBridge       RootPath  DesignatedBridge Root  Max Hel Fwd
Identifier       Cost      Identifier       Port  Age lo  Dly
hex                        hex                    sec sec sec
80000024388f6b00 2         80000024388f6b00 3/1   20  2   15
STP Port Parameters:
Port  Prio Path      State      Designat- Designated       Designated
Num   rity Cost                ed Cost   Root             Bridge
3/2   128  2         BLOCKING   0         80000024388f6b00 80000024388f6b00
3/3   128  2         BLOCKING   0         80000024388f6b00 80000024388f6b00
3/4   128  2         BLOCKING   0         80000024388f6b00 80000024388f6b00
```

History

Release	Command History
5.5.00	The command was modified to display only ports blocked by the Spanning Tree Protocol.

show statistics

Displays the statistics for a specific option.

Syntax

show statistics brief [*ethernet* | *lag* | *management* | *pos* | *slot* | *tunnel*]

show statistics dos-attack

show statistics ethernet *slot/port*

show statistics lag *lag_name*

show statistics management *dec*

show statistics pos *slot/port*

show statistics slot *dec*

show statistics tunnel *tunnel-id*

show statistics ipsec-tunnel *tunnel-id*

Parameters

brief

Displays the port statistics in brief mode.

ethernet

Displays the ethernet port in brief mode.

lag

Displays LAG in brief mode.

management

Displays the management port in brief mode.

pos

Displays the POS port in brief mode.

slot

Displays all ports in a slot in brief mode.

tunnel

Displays IP tunnel statistics in brief mode.

dos-attack

Displays DOS-attack statistics.

ethernet *slot/port*

Displays the ethernet port for the specified slot and port.

lag

Displays LAG determined by the *lag_name* variable.

management

Displays the management port determined by the *dec* variable.

pos
Displays the POS port determined by the *slot/port* variable.

slot
Displays all of the ports in a slot determined by the *slot/port* variable.

tunnel
Displays the IP tunnel statistics determined by the *tunnel-id* variable.

ipsec-tunnel *tunnel-id*
Displays the bytes and packets count for the specified IPSec tunnel ID.

Modes

This command operates under all modes.

Command Output

The **show statistics** *ethernet* command displays the following information:

Output field	Description
InOctets	The total number of good octets and band octets received.
OutOctets	The total number of good and bad octets transmitted.
InPkts	The total number of packets received. the count includes rejected and local packets that are not transmitted to the switching core for transmission.
OutPkts	The number of good packets received. The count includes unicast, multicast, and broadcast packets.
InBroadcastPkts	The total number of good broadcast packets received.
OutBroadcastPkts	The total number of good broadcast packets transmitted.
InMulticastPkts	The total number of good multicast packets received.
OutMulticastPkts	The total number of good multicast packets transmitted.
InUnicastPkts	The total number of good unicast packets received.
OutUnicastPkts	The total number of good unicast packets transmitted.
InDiscards	The total number of packets that were received and then dropped due to a lack of received buffers.
OutDiscards	The total number of packets that were transmitted and then dropped due to a lack of transmit buffers.
InErrors	The total number of packets received that had Alignment errors or phy errors.
OutErrors	The total number of packets transmitted that has Alignment errors or phy errors.
InCollisions	The total number of packets received in which a Collision event was detected.
OutCollisions	The total number of packets transmitted in which a Collision event was detected.
OutLateCollisions	The total number of packets transmitted in which a Collision event was detected but for which a *receive error (RX error)* event was not detected.
Alignment	The total number of packets received that were from 64 - 1518 octets long but had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (Alignment error).
FCS	The Frame Checksum error.
InFlowCtrlPkts	The total number of ingress flow control packets. "N/A" indicates that the interface module does not support flow control statistics.

Output field	Description
OutFlowCtrlPkts	The total number of egress flow control packets.
GiantPkts	The total number of packets for which all of the following is true: • The data length was longer than the maximum allowable frame size. • No Rx error was detected.
ShortPkts	The total number of packets received for which all of the following is true: • The data length was less than 64 bytes. • No Rx error was detected. • No Collision or late Collision was detected.
InBitsPerSec	The number of bits received per second.
OutBitsPerSec	The number of bits transmitted per second.
InPktsPerSec	The number of packets received per second.
OutPktsPerSec	The number of packets transmitted per second.
InUtilization	The percentage of the port's bandwidth used by received traffic.
OutUtilization	The percentage of the port's bandwidth used by transmitted traffic.

The **show statistics tunnel** command displays the following information:

This field...	Displays...
Tunnel ID	For each tunnel displayed, the Tunnel ID indicates the tunnel for which the statistics are displayed.
Tunnel Type	The tunnel type is either GRE or manual IPv6.
In-ports	The Ethernet ports traversed by the tunnel.
Packets Rcv-from-tnnl	The number of packets that have arrived from the tunnel.
Packets Xmit-to-tnnl	The number of packets that have been sent to the tunnel.

Examples

The following example displays the **show statistics ethernet** command:

```
device# show statistics ethernet 9/1


PORT 9/1 Counters:
InOctets          210753498112    OutOctets          210753550720
InPkts            1646511726      OutPkts            1646512119
InBroadcastPkts   0               OutBroadcastPkts   0
InMulticastPkts   0               OutMulticastPkts   0
InUnicastPkts     1646511726      OutUnicastPkts     1646512142
InDiscards        0               OutDiscards        0
InErrors          0               OutErrors          0
InCollisions      0               OutCollisions      0
                                  OutLateCollisions  0
Alignment         0               FCS                0
InFlowCtrlPkts    0               OutFlowCtrlPkts    0
GiantPkts         0               ShortPkts          0
InBitsPerSec      3440829770      OutBitsPerSec      3440686411
InPktsPerSec      3360185         OutPktsPerSec      3360085
InUtilization     39.78%          OutUtilization     39.78%
```

The following example displays output from the **show statistics tunnel** command with a specific *tunnel-id* option. In this example, the tunnel type is GRE.

NOTE
When reviewing the keepalive packet statistics in the output of the show interface tunnel command for a GRE tunnel, note that the transmitted keepalive packets are hardware generated and are not counted in the "Rcv-from-tnnl" and "Xmit-to-tnnl" statistics.

```
device# show statistics tunnel 1
                                              Packets
Tunnel Id  Tunnel Type  In-Port(s)     [Rcv-from-tnnl   Xmit-to-tnnl]
1          GRE          e2/1 - e2/2    586046           287497
                        e2/3 - e2/4    100340           150034
```

The following example displays the **show statistics brief ipsec-tunnel** command modified to display IPsec tunnel interface packet and byte count.

```
device#show statistics brief ipsec-tunnel
#    Tnnl       RxPkts     RxBytes         TxPkts     TxBytes
 1    24         0          0               0          0
 2    100        0          0               457        79518
 3    101        0          0               0          0
 4    102        0          0               0          0
 5    103        0          0               1          174
 6    104        0          0               0          0
 7    105        0          0               0          0
 8    106        0          0               0          0
 9    107        0          0               0          0
 10   108        0          0               0          0
 11   109        0          0               0          0
 12   110        0          0               0          0
 13   123        0          0               0          0
 14   124        0          0               0          0
 15   125        0          0               0          0
 16   150        0          0               0          0
 17   254        0          0               0          0
```

The following example shows the bytes and packet count only for the IPSec tunnel interface 100.

```
device# show statistics ipsec-tunnel 100

IPSec tunnel 100 statistics:
  RxPkts:       0                     TxPkts:   467
  RxBytes:      0                     TxBytes:  81258
```

History

Release version	Command history
05.8.00	This command was modified to display IPsec tunnel interface packet and byte count.

show sysmon config

Displays the system monitoring configuration.

Syntax

show sysmon config

Modes

User EXEC mode

Command Output

The **show sysmon config** command displays the following information:

Output field	Description
EVENT	Name of the diagnostic test.
ACTION	Action to be taken in case of a failure of the test.
POLL PERIOD (SEC)	The polling period in seconds.
THRESHOLD #(PER POLL in #POLL)	The number of failed tests out of the number of pollings (applicable only for threshold based test).
LOG BACK-OFF	The number of event logs to be skipped before logging again.

Examples

The following example displays the monitoring configuration.

```
device# show sysmon config
--------------------------+----------------+-----------+----------+------------
EVENT                     | ACTION         |POLL PERIOD|THRESHOLD|LOG BACK-OFF
                          |                |   (SEC)   |#(PER POLL|
                          |                |           | in #POLL)|
--------------------------+----------------+-----------+----------+------------
TM. Link Monitoring       |SHUTDOWN-LINK   |    60     | 5 in 10  |  1800
--------------------------+----------------+-----------+----------+------------
Port CRC Monitoring       |SYSLOG          |    60     | 3 in 5   |  1800
--------------------------+----------------+-----------+----------+------------
FE. Link Monitoring       |SHUTDOWN-LINK   |    60     | 5 in 10  |  1800
--------------------------+----------------+-----------+----------+------------
NP Memory Error Monitoring |SYSLOG-AND-TRAP |    10     |   N/A    |  N/A
--------------------------+----------------+-----------+ ---------+------------
```

History

Release Version	Command History
5.6.00	This command was modified to display the NP memory error monitoring event configuration.

show sysmon results brief

Displays summary information of scheduled test results in brief without providing the instance information.

Syntax

show sysmon results *test-name* **brief**

Parameters

test-name

Displays summary results for a specific scheduled test.

Modes

User EXEC mode

Command Output

The **show sysmon results brief** command displays the following information:

Output field	Description
EVENT	Name of the diagnostic test.
ACTION	Action to be taken in case of a failure of the test.
SLOTS	Slots on which the test is configured to run.
MODE	Mode of running for the test. The modes are Continuously polling or Scheduling.
POLL PERIOD (SEC)	The polling period in seconds.
THRESHOLD #(PER POLL in #POLL)	The number of failed tests out of the number of pollings (applicable only for threshold based test).
LOG BACK-OFF	The number of event logs to be skipped before logging again.
SLOT	The slot number.
TEST TYPE	The specific scheduling test type.
BRIEF RESULT (LAST RUN/CYCLE)	The brief results showing only the status (passed/ failed) of the test on each slot.

Examples

The following example displays results from the port-crc-test.

```
device(config)#show sysmon results port-crc-test brief
Module is(are) not UP in slot(s) 3 4 5
The configuration of port-crc-test is
-------------------------+---------------------+----------+----------+-----------+------------
+-----------
EVENT                    |ACTION               |SLOTS     |MODE      |POLL PERIOD| THRESHOLD  |LOGBACK-
OFF
                         |                     |          |          |   (SEC)   | #(PER POLL
|
                         |                     |          |          |           |  in #POLL)
|
-------------------------+---------------------+----------+----------+-----------+------------
+-----------
Port CRC Monitoring      |SYSLOG               |ALL       |SCHEDULING|     60    |   3 in 4   |   1
-------------------------+---------------------+----------+----------+-----------+------------
+-----------
Brief result of port-crc-test is
---------+----------------------------------------+-------------------------------------
  SLOT   |           TEST TYPE                    |    BRIEF RESULT (LAST RUN/CYCLE)
---------+----------------------------------------+-------------------------------------
 Slot 1  |   Scheduled at  2014.05.27-10:56:52    |         PASSED
---------+----------------------------------------+-------------------------------------
 Slot 2  |   Scheduled at  2014.05.27-10:56:52    |         PASSED
---------+----------------------------------------+-------------------------------------
 Slot 6  |   Scheduled at  2014.05.27-10:56:52    |         PASSED
---------+----------------------------------------+-------------------------------------
 Slot 7  |   Scheduled at  2014.05.27-10:56:52    |         PASSED
---------+----------------------------------------+-------------------------------------
 Slot 8  |   Scheduled at  2014.05.27-10:56:52    |         PASSED
---------+----------------------------------------+-------------------------------------
```

History

Release version	Command history
05.7.00	This command was introduced.

show sysmon results detail

Displays scheduled test results in detail for a specified slot. Instance information and other details are displayed.

Syntax

show sysmon results *test-name* **detail** *slot-id*

Parameters

test-name

Displays detailed results for specified test name.

slot-id

Displays detailed results for a specified slot name of theThe slot numbers to be specified to run the test.

Modes

User EXEC mode

Command Output

The **show sysmon results detail** command displays the following information:

Output field	Description
EVENT	Name of the diagnostic test.
ACTION	Action to be taken in case of a failure of the test.
SLOTS	Slots on which the test is configured to run.
MODE	Mode of running for the test. The modes are Continuously polling or Scheduling.
POLL PERIOD (SEC)	The polling period in seconds.
THRESHOLD #(PER POLL in #POLL)	The number of failed tests out of the number of pollings (applicable only for threshold based test).
LOGBACK-OFF	The number of event logs to be skipped before logging again.
INSTANCE	
TEST TYPE	The specific scheduling test type.
# OF RUNS	The number of times test is run.
# OF FAILURES	The number of times the test failed (out of the number of runs).

Examples

The following example displays information about the port-crc-test.

```
device(config)#show sysmon results port-crc-test detail 1
The configuration of port-crc-test is
---------------------------+--------------------+-------------+----------+-----------+------------
+-----------
EVENT                      |ACTION              |SLOTS        |MODE      |POLL PERIOD| THRESHOLD  |
LOGBACK-OFF
                           |                    |             |          |   (SEC)   | #(PER POLL
|
                           |                    |             |          |           |  in #POLL)
|
---------------------------+--------------------+-------------+----------+-----------+------------
+-----------
Port CRC Monitoring        |SYSLOG              |ALL          |SCHEDULING|     60    |   3 in 4   |
1
---------------------------+--------------------+-------------+----------+-----------+------------
+-----------
The detail result (LAST RUN/CYCLE) of port-crc-test on LP 1 is
------------------+-------------------------------------+---------+---------
     INSTANCE     |             TYPE                    |  # OF   | # OF
                  |                                     |  RUNS   | FAILURES
------------------+-------------------------------------+---------+---------
       Port 1/1   | Scheduled at  2014.05.27-10:56:52 |    4    |   0
------------------+-------------------------------------+---------+---------
       Port 1/2   | Scheduled at  2014.05.27-10:56:52 |    4    |   0
------------------+-------------------------------------+---------+---------
       Port 1/3   | Scheduled at  2014.05.27-10:56:52 |    4    |   0
------------------+-------------------------------------+---------+---------
       Port 1/4   | Scheduled at  2014.05.27-10:56:52 |    4    |   0
------------------+-------------------------------------+---------+---------
```

History

Release version	Command history
05.7.00	This command was introduced.

show sysmon schedule

Displays details of scheduled tests.

Syntax

show sysmon sched *name of the test*

Parameters

name of the test

The name of the scheduled test.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show sysmon schedule** command displays the following information:

Output field	Description
TEST NAME	Name of the test.
SCHEDULED AT	The scheduled time in hh:mm:ss mm-dd-yy format. Here the first instance of mm is minutes and the second instance is months. For example, 14:30:00 08-20-13.
MP/LP	Type of slot.
# OF RUNS	The number of runs. The range is between 1 and 31.
THRESHOLD	Threshold value of the diagnostic test.
TEST INTERVAL (SEC)	The test interval value in seconds.

Examples

The following example displays information about the port-crc-test.

```
device(config)#show sysmon schedule port-crc-test
--------------------------+----------------------+-----+-----------+------------+-----------
         TEST NAME        |  SCHEDULED           |MP/LP|  # OF     |  THRESHOLD |   TEST
                          |     AT               |     |   RUNS    |            |  INTERVAL
                          |                      |     |           |            |   (SEC)
--------------------------+----------------------+-----+-----------+------------+-----------
Port CRC Monitoring       |    2014.05.23-06:39:28|   LP|     4     |      3     |     60
--------------------------+----------------------+-----+-----------+------------+-----------
```

The following example displays information about the np-memory-errors test.

```
device(config)#show sysmon schedule np-memory-errors
---------------------------+----------------------+-----+-----------+------------+-----------
         TEST NAME         |  SCHEDULED           |MP/LP|  # OF     |  THRESHOLD |   TEST
                           |     AT               |     |   RUNS    |            |  INTERVAL
                           |                      |     |           |            |   (SEC)
---------------------------+----------------------+-----+-----------+------------+-----------
NP Memory Error Monitoring |    2014.05.23-06:39:34|   LP|     4     |      0     |     60
---------------------------+----------------------+-----+-----------+------------+-----------
```

History

Release version	Command history
05.7.00	This command was introduced.

show telemetry

Displays information related to the telemetry configuration.

Syntax

show telemetry [**detail**] **rule-name** *rule-name*

Parameters

detail

Displays detailed information. The list of ports will be fully expanded and displayed if the ports are LAG or VLAN ports.

rule-name *rule-name*

Displays specified rule name information.

Modes

EXEC mode

Usage Guidelines

Examples

The following example displays the UDA PBR policy detail along with the IPv4, IPv6 PBR information.

```
device(config)# show telemetry detail rule-name
Rule name: default-rulename
Input: IPv4 - 1/1
Route-map Policy: Test2
IPv4 ACL match:  110
Output:
Input: IPv4 - 3/1
Route-map Policy: Test1
IPv4 ACL match:  100
Output:
Input: UDA - 3/1
Route-map Policy: Test1
UDA ACL match:  2000
Output:
```

The following example displays the UDA PBR policy detail along with the IPv4, IPv6 and PBR information.

```
device(config)# show telemetry rule-name
Paths with leading * are configured but disabled, entries with + are for IPv6 entries with # are for UDA
                              Route-map    ACL         Output   Output
Name              Input       Policy       Match       VLAN     Port(s)/IP
RT_TEST1          4/8         Test1                    100
+RT_TEST1         4/8         Test1                    100
#RT_TEST1         4/8         Test1                    100
*RT_TEST3         N/A         Test3                    N/A      N/A
#RT_TEST4         3/3         Test4                             2/3
```

Release version	Command history
5.9.00	This command was modified to display the UDA PBR policy detail along with the IPv4, IPv6 PBR information.

show terminal

Displays terminal settings.

Syntax

show terminal

Modes

User EXEC mode

Command Output

The **show terminal** command displays the following information:

Output field	Description
2015-08-11T22:20:59+00:00	Timestamp is displayed in ISO 8601 format: YYYY-MM-DDThh:mm:ssTZD (for example, 1997-07-16T19:20:30+01:00).
Length	Number of lines configured as the terminal length.
Page display mode (session)	Session page display is either enabled or disabled.
Page display mode (global)	Global page display is either enabled or disabled.
Timestamp: enabled	The format in which the timestamp is displayed; system or iso8601.

Examples

The following example displays the terminal settings.

```
device# show terminal

Length: 24 lines
Page display mode (session): disabled
Page display mode (global): enabled
Timestamp: enabled (system format)
```

The following example displays the terminal settings with a timestamp and iso8601 format.

```
device# show terminal

2015-08-11T22:20:59+00:00
Length: 24 lines
Page display mode (session): disabled
Page display mode (global): enabled
Timestamp: enabled (iso8601 format)
```

History

Release version	Command history
05.4.0	This command was introduced.
05.9.0	This command was modified to include timestamp information in ISO 8601 format.

show tm-voq-stat queue-drops

Use **show tm-voq-stat queue-drops** command to display traffic manager statistics.

Syntax

show tm-voq-stat queue-drops dst_port *destination-port* **ethernet** *slot/port*

Modes

This command operates in the Global configuration mode.

Command Output

The **show tm-voq-stat queue-drops** command displays the following information:

TABLE 15 Traffic Manager statistics for queue drops

This field...	Displays...
EnQue Pkt Count	A count of all packets entering ingress queues on this traffic manager.
EnQue Byte Count	A count of all bytes entering ingress queues on this traffic manager.
DeQue Pkt Count	A count of all packets dequeued from ingress queues and forwarded on this traffic manager.
DeQue Byte Count	A count of all bytes dequeued from ingress queues and forwarded on this traffic manager.
TotalQue Discard Pkt Count	A count of all packets failing to enter ingress queues on this traffic manager. This may be due to: • the queue reaching its maximum depth, WRED, or other reasons. • the network processor deciding to drop packets for reasons including: an unknown Layer-3 route, RPF, or segment filtering.
TotalQue Discard Byte Count	A count of all bytes failing to enter ingress queues on this traffic manager. This may be due to: • the queue reaching its maximum depth, WRED, or other reasons. • the network processor deciding to drop packets for reasons including: an unknown Layer-3 route, RPF, or segment filtering.

History

Release version	Command history
NI 5.7.00 release	This command was introduced .

show tvf-domain

Displays transparent VLAN flooding (TVF) domain information.

Syntax

show tvf-domain [*tvf-domain-ID* | **brief** | **detail** | **ethernet** *slot/port*]

Parameters

tvf-domain-ID
Displays the information of a specific TVF domain.

brief
Displays a brief summary of all the configured TVF domains.

detail
Displays detailed information of each TVF domain.

ethernet *slot/port*
Displays the details of the port configured in the VLAN.

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

TVF domain configuration mode

Command Output

The **show tvf-domain** command displays the following information:

Output field	Description
TVF FID pool size	FID pool size configured for TVF LAG load balancing.
Max FID groups	Maximum number of FID groups.
FID group size	FID group size configured for TVF LAG load balancing.
TVF domain memory usage	Transparent VLAN flooding memory usage.
Per entry usage	Memory usage for each entry.
TVF Domain ID	ID of the TVF domain.
Name	Name of the TVF domain
Ports	Ports configured in the VLAN.
Type	Type of ports.
Protocol	Supported protocols. Value is NONE as protocol support is not added.
State	Status of the port.
Group ID	LAG trunk ID.

Output field	Description
FID Base	Base FID value allocated for a particular TVF domain or VLAN.
FID Count	Number of FIDs used starting from the base FID. This depends on the maximum trunk group count.

Examples

The following example displays information about the TVF domain.

```
device(config)# show tvf-domain
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 2048, FID group size: 2
2047 (VLAN 32, TVF Domain 2015) TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done

TVF domain memory usage : 735848 bytes
Per entry usage         : 365 bytes

TVF Domain ID 1, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 2, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 3, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 4, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 6, Name [None]
Ports : ethe 8/5 to 8/8
```

The following example displays the information of a specific TVF domain.

```
device(config)# show tvf-domain 1
TVF Domain ID 1, Name [None]
Ports : ethe 8/5 to 8/8
------------------------------------------------------------
Port  Type      Protocol  State
8/5   TRUNK     NONE      UP
8/6   TRUNK     NONE      UP
8/7   TRUNK     NONE      UP
8/8   TRUNK     NONE      UP
Group ID: 33, FID Base 0x00009ffe, FID Count 2
tvf_lag_lb_fid0: 0x00009ffe, mask ethe 8/5 ethe 8/7
tvf_lag_lb_fid1: 0x00009fff, mask ethe 8/6 ethe 8/8
```

The following example displays a brief summary of all the configured TVF domains.

```
device(config)# show tvf-domain brief
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 2048, FID group size: 2
2047 (VLAN 32, TVF Domain 2015) TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done

TVF domain memory usage : 735848 bytes
Per entry usage         : 365 bytes
TVF   Name       Ports
----- ----       -----
1     [None]     Ports : ethe 8/5 to 8/8
2     [None]     Ports : ethe 8/5 to 8/8
3     [None]     Ports : ethe 8/5 to 8/8
4     [None]     Ports : ethe 8/5 to 8/8
6     [None]     Ports : ethe 8/5 to 8/8
7     [None]     Ports : ethe 8/5 to 8/8
8     [None]     Ports : ethe 8/5 to 8/8
9     [None]     Ports : ethe 8/5 to 8/8
10    [None]     Ports : ethe 8/5 to 8/8
11    [None]     Ports : ethe 8/5 to 8/8
12    [None]     Ports : ethe 8/5 to 8/8
13    [None]     Ports : ethe 8/5 to 8/8
14    [None]     Ports : ethe 8/5 to 8/8
15    [None]     Ports : ethe 8/5 to 8/8
16    [None]     Ports : ethe 8/5 to 8/8
17    [None]     Ports : ethe 8/5 to 8/8
18    [None]     Ports : ethe 8/5 to 8/8
19    [None]     Ports : ethe 8/5 to 8/8
20    [None]     Ports : ethe 8/5 to 8/8
21    [None]     Ports : ethe 8/5 to 8/8
22    [None]     Ports : ethe 8/5 to 8/8
23    [None]     Ports : ethe 8/5 to 8/8
24    [None]     Ports : ethe 8/5 to 8/8
25    [None]     Ports : ethe 8/5 to 8/8
26    [None]     Ports : ethe 8/5 to 8/8
27    [None]     Ports : ethe 8/5 to 8/8
28    [None]     Ports : ethe 8/5 to 8/8
29    [None]     Ports : ethe 8/5 to 8/8
30    [None]     Ports : ethe 8/5 to 8/8
31    [None]     Ports : ethe 8/5 to 8/8
32    [None]     Ports : ethe 8/5 to 8/8
33    [None]     Ports : ethe 8/5 to 8/8
34    [None]     Ports : ethe 8/5 to 8/8
35    [None]     Ports : ethe 8/5 to 8/8
36    [None]     Ports : ethe 8/5 to 8/8
37    [None]     Ports : ethe 8/5 to 8/8
```

The following example displays detailed information of each TVF domain.

```
device(config)# show tvf-domain detail
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 2048, FID group size: 2
2047 (VLAN 32, TVF Domain 2015) TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done

TVF domain memory usage : 735848 bytes
Per entry usage         : 365 bytes

TVF Domain ID 1, Name [None]
Ports : ethe 8/5 to 8/8
-----------------------------------------------------------
Port  Type      Protocol  State
8/5   TRUNK     NONE      UP
8/6   TRUNK     NONE      UP
8/7   TRUNK     NONE      UP
8/8   TRUNK     NONE      UP
Group ID: 34, FID Base 0x00009ffe, FID Count 2

TVF Domain ID 2, Name [None]
Ports : ethe 8/9 to 8/12
-----------------------------------------------------------
Port  Type      Protocol  State
8/9   TRUNK     NONE      UP
8/10   TRUNK     NONE      UP
8/11   TRUNK     NONE      UP
8/12   TRUNK     NONE      UP
Group ID: 33, FID Base 0x00009ffe, FID Count 2
```

The following example displays the details of the port configured in the TVF domain.

```
device(config)# show tvf-domain ethernet 8/6
TVF Domain : 1
TVF Domain : 2
TVF Domain : 3
TVF Domain : 4
TVF Domain : 6
TVF Domain : 7
TVF Domain : 8
TVF Domain : 9
TVF Domain : 10
TVF Domain : 11
TVF Domain : 12
TVF Domain : 13
TVF Domain : 14
TVF Domain : 15
TVF Domain : 16
TVF Domain : 17
TVF Domain : 18
TVF Domain : 19
TVF Domain : 20
TVF Domain : 21
TVF Domain : 22
TVF Domain : 23
TVF Domain : 24
```

History

Release version	Command history
6.0.00	This command was introduced.

show vlan

Displays VLAN information.

Syntax

show vlan *vlan_id* [**statistics**]

show vlan *vlan_id* **brief** [**wide**]

show vlan *vlan_id* [**statistics**] **detail**

show vlan *vlan_id* [**statistics**] **ethernet** [*slot/port*]

show vlan *vlan_id* [**statistics**] **tvf-lag-lb** [**detail**]]

Parameters

vlan_id

VLAN identifier.

statistics

Displays VLAN extended counters.

brief

Displays VLAN information in table format.

wide

Displays full VLAN name.

detail

Displays VLAN information in a detailed format.

ethernet *slot/port*

Port configured in the VLAN.

tvf-lag-lb

Displays transparent VLAN flooding load balancing information

detail

Displays transparent VLAN flooding load balancing information in detail.

Modes

Privileged EXEC mode.

Examples

The following example displays transparent VLAN flooding LAG load balancing information.

```
device# show vlan tvf-lag-lb
****TVF LAG Load Balancing****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 2048, Max FID groups: 512, FID group size: 4
TVF LAG Load balancing groups:
VLAN: 100, group ID: 257, FID base: 0x9800, FID count: 4
VLAN: 200, group ID: 258, FID base: 0x9804, FID count: 4
2TVF LAG Load balancing groups are configured
```

The following example displays the full VLAN name and information in table format.

```
device# show vlan brief wide

Configured PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 512
Default PORT-VLAN id: 1

VLAN  Name              Ports
----  ----              -----
1     DEFAULT-VLAN      Untagged Ports : ethe 4/1 to 4/8
100   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 4/1 to 4/8
                        Untagged Ports : ethe 3/1 to 3/24
200   [None]            Statically tagged Ports: ethe 3/1 to 3/24 ethe 4/1 to 4/8
                        Untagged Ports : ethe 1/1 to 1/2
300   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
400   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
500   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
600   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
700   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
800   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
900   [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
1000  [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
2000  [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
3000  [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
4000  [None]            Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8
4090  [None]
4095  CONTROL-VLAN
```

History

Release version	Command history
5.6.00	This command is modified to include the **tvf-lag-lb** parameter.
5.8.00	This command is modified to include the **brief wide** parameter.

show vlan tvf-lag-lb

Displays transparent VLAN flooding LAG load balancing information.

Syntax

show vlan tvf-lag-lb detail

Parameters

detail

Specifies the detailed VLAN flooding LAG load balancing information in the output.

Modes

Privileged EXEC mode

Usage Guidelines

The **show vlan tvf-lag-lb** command displays transparent VLAN flooding LAG load balancing information.

Examples

The following example displays transparent VLAN flooding LAG load balancing information:

```
device#show vlan tvf-lag-lb
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 1024, FID group size: 4
2 TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done
```

The following example displays the detailed transparent VLAN flooding LAG load balancing information:

```
device#show vlan tvf-lag-lb detail
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 1024, FID group size: 4
2 TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done


TVF LAG Load balancing groups:
VLAN: 100, group ID: 33, FID base: 0x9ffc, FID count: 4
VLAN: 200, group ID: 34, FID base: 0x9ff8, FID count: 4
```

History

Release	Command History
5.6.00	This command was introduced.
5.9.00	This command was modified to include additional information in the command output.

show vsrp

Displays the VSRP information.

Syntax

show vsrp [**aware**] [**vlan** *vlan-id* [*vrid-num*] | **vrid** *vrid-num*]

show vsrp [**brief**]

show vsrp [**statistics** [**vlan** *vlan-id*]]

Parameters

aware
Displays information about VSRP-aware devices.

vlan *vlan-id*
Displays VSRP information for the VLAN ID.

vrid *vrid-num*
Displays information for the ports with VSRP enabled.

brief
Displays the VSRP information summary.

statistics
Displays the global VSRP statistics.

Modes

User EXEC mode

Command Output

The **show vsrp** command displays the following information:

Output field	Description
Total number of VSRP routers defined	The total number of VRIDs configured on this device.
VLAN	The VLAN on which VSRP is configured.
auth-type	The authentication type in effect on the ports in the VSRP VLAN.
VRID	The VRID for which the VSRP information is displayed.
state	The device VSRP state for the VRID. The state can be one of the following: • initialize: The VRID is not enabled (activated). If the state remains "initialize" after you activate the VRID, make sure that the VRID is also configured on the other routers and that the routers can communicate with each other. • standby: This device is a backup for the VRID. • master: This device is the master for the VRID.
Administrative-status	The administrative status of the VRID. The administrative status can be one of the following: • disabled: The VRID is configured on the interface but VSRP or VRRP-E has not been activated on the interface.

Output field	Description
	• enabled: VSRP has been activated on the interface.
Advertise-backup	Whether the device is enabled to send VSRP Hello messages when it is a backup. This field can have one of the following values: • disabled: The device does not send Hello messages when it is a backup. • enabled: The device sends Hello messages when it is a backup.
Preempt-mode	Whether the device can be preempted by a device with a higher VSRP priority after this device becomes the master. This field can have one of the following values: • disabled: The device cannot be preempted. • enabled: The device can be preempted.
Configured	Indicates the parameter value configured on this device.
Current	Indicates the parameter value received from the master.
Unit	Indicates the formula used tor calculating the VSRP priority and the timer scales in effect for the VSRP timers. A timer true value is the value listed in the Configured or Current field divided by the scale value.
priority	The device preferability for becoming the master for the VRID. During negotiation, the backup with the highest priority becomes the master. If two or more backups are tied with the highest priority, the backup interface with the highest IP address becomes the master for the VRID.
hello-interval	The number of seconds between Hello messages from the master to the backups for a given VRID.
dead-interval	The configured value for the dead interval. The dead interval is the number of seconds a backup waits for a Hello message from the master for the VRID before determining that the master is no longer active. If the master does not send a Hello message before the dead interval expires, the backups negotiate (compare priorities) to select a new master for the VRID. If the value is 0, then you have not configured this parameter.
hold-interval	The number of seconds a backup that intends to become the master will wait before actually beginning to forward Layer 2 traffic for the VRID. If the backup receives a Hello message with a higher priority than its own before the hold-down interval expires, the backup remains in the backup state and does not become the new master.
initial-ttl	The number of hops a Hello message can traverse after leaving the device before the Hello message is dropped. A metro ring counts as one hop, regardless of the number of nodes in the ring.
next hello sent in	The amount of time until the master dead interval expires. If the backup does not receive a Hello message from the master by the time the interval expires, either the IP address listed for the master will change to the IP address of the new master, or this Layer 3 switch itself will become the master. This field applies only when this device is a backup.
master router	The IP address of the master router.
Member ports	The ports in the VRID.
Operational ports	The member ports that are currently up.
Forwarding ports	The member ports that are currently in the forwarding state. Ports that are forwarding on the master are listed. Ports on the Standby, which are in the blocking state, are not listed.

The **show vsrp aware** command displays the following information:

Output field	Description
Last Port	The most recent active port connection to the VRID. This is the port connected to the current master. If a failover occurs, the VSRP-aware device changes the port to the port connected to the new master. The VSRP-aware device uses this port to send and receive data through the backed-up node.

Examples

The following example shows the output of the **show vsrp aware** command.

```
device# show vsrp aware
Aware port listing
VLAN ID        VRID        Last Port
100               1              3/2
200               2              4/1
```

The following example shows the output of the **show vsrp vlan** *vlan-id* **vrid** *vrid-num* command.

```
device# show vsrp vlan 100 vrid 100
VLAN 100
auth-type no authentication
VRID 100
========
State        Administrative-status        Advertise-backup    Preempt-mode
master        enabled                        disabled            true
Parameter             Configured        Current        Unit/Formula
priority              100                    50               (100-0)*(2.0/4.0)
hello-interval     1                       1                 sec/1
dead-interval      3                       3                 sec/1
hold-interval      3                       3                 sec/1
initial-ttl           2                       2                 hops
next hello sent in 00:00:00.3
Member ports:      ethe 2/5 to 2/8
Operational ports: ethe 2/5 ethe 2/8
Forwarding ports:  ethe 2/5 ethe 2/8
Restart ports:     2/5(1) 2/6(1) 2/7(1) 2/8(1)
```

Commands Si - Z

slow-start

Configures a slow-start timer interval to extend the time interval beyond the dead-interval time before a Virtual Router Redundancy Protocol Extended (VRRP-E) master device assumes the role of master device after being offline. When the original master device went offline, a backup VRRP-E device with a lower priority became the master device.

Syntax

slow-start *seconds* [**use-track-port** [**restart**]]

no slow-start *seconds* [**use-track-port** [**restart**]]

Command Default

If a slow-start timer is not configured, the master device assumes control from a backup device immediately after the dead interval.

Parameters

seconds

Sets the number of seconds for the slow-start timer. Range from 1 through 57600.

use-track-port

Implements a slow-start timer for the first tracked port "up" state change, in addition to the VRRP-E initialization state.

restart

Restarts the slow-start timer for subsequent tracked port "up" state changes after the initial tracked port state change.

Modes

VRRP-E router configuration mode

Usage Guidelines

When the VRRP-E slow-start timer is enabled, if the master VRRP-E device goes down, the backup device with the highest priority takes over after the expiration of the dead interval. If the original master device subsequently comes back up again, the amount of time specified by the VRRP-E slow-start timer elapses before the original master device takes over from the backup device (which became the master device when the original master device went offline).

The slow-start allows for protocol convergence and can also be used for tracked port state changes. If the **use-track-port** option is not configured, the slow-start timer will be started only for the VRRP-E master device initialization, not for any tracked port state change.

This command is supported only for VRRP-E.

The **no** form removes the slow-start configuration.

Examples

The following example sets the slow-start timer interval to 30 seconds and configures the slow-start timer to run when a tracked port changes state.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# slow-start 30 use-track-port restart
```

slow-start

Configures the VSRP slow start timer, which causes a specified amount of time to elapse between the time the Master is restored and when it takes over from the Backup.

Syntax

slow-start *timer*

no slow-start *timer*

Command Default

By default, the slow start timer is not configured and the transition from Backup back to Master takes place immediately.

Parameters

timer

Configures the VSRP slow start time. The range is from 1 to 600 ticks (1/10 second to 60 seconds).

Modes

VSRP router configuration mode

Usage Guidelines

In a VSRP configuration, if a Master router goes down, the Backup router with the highest priority takes over. When the Master comes back up again, it takes over from the Backup. By default, this transition from Backup back to Master takes place immediately. You can configure the VSRP slow start timer feature, which causes a specified amount of time to elapse between the time the Master is restored and when it takes over from the Backup. (This range is currently set to between 1 to 600 ticks (1/10 second to 60 seconds). This interval allows time for VSRP convergence when the Master is restored.

When the VSRP slow start timer is enabled, if the Master goes down, the Backup takes over immediately. If the Master subsequently comes back up again, the amount of time specified by the VSRP slow start timer elapses (in this example, 30 seconds) before the Master takes over from the Backup.

The **no** form of the command removes the VSRP slow start timer.

Examples

The following example configures the VSRP slow start timer ro 30 seconds.

```
device(config)# router vsrp
device(config-vsrp-router)# slow-start 300
```

snmp-server community

Configures the SNMP community string and access privileges.

Syntax

snmp-server community *community-string* { **ro** | **rw** } [*acl-name* | *acl-num* | **ipv6** *ipv6-acl-name* | **view** [*mib-view*]]

no snmp-server community *community-string* { **ro** | **rw** } [*acl-name* | *acl-num* | **ipv6** *ipv6-acl-name* | **view** [*mib-view*]]

Command Default

The SNMP community string is not configured.

Parameters

community-string
: Configures the SNMP community string that you must enter to gain SNMP access. The string is an ASCII string and can have up to 32 characters.

ro
: Configures the community string to have read-only ("get") access.

rw
: Configures the community string to have read-write ("set") access.

acl-name
: Filters incoming packets using a named standard access control list (ACL).

acl-num
: Filters incoming packets using a numbered ACL.

ipv6 *ipv6-acl-name*
: Filters incoming packets using a named IPv6 ACL.

view *mib-view*
: Associates a view to the members of the community string. Enter up to 32 alphanumeric characters.

Modes

Global configuration mode

Usage Guidelines

The **view** *mib-view* parameter allows you to associate a view to the members of this community string. If no view is specified, access to the full MIB is granted. The view that you want must exist before you can associate it to a community string.

You can set just one access type, either read-only (ro) or read/write (rw) for a single SNMP community instead of setting both access types. The read/write access supersedes read-only configuration and if read/write is configured for a specified community after read only, the running configuration file only saves the rw configuration line.

If you issue the **no snmp-server community public ro** command and then enter the **write memory** command to save the configuration, the read-only "public" community string is removed and will have no SNMP access. If for some reason the device is brought down and then brought up, the **no snmp-server community public ro** command is restored in the system and the read-only "public" community string has no SNMP access.

The **no** form of the command removes an SNMP community string.

Examples

The following example configures an SNMP community string with read-only access.

```
device# configure terminal
device(config)# snmp-server community private ro
```

The following example configures an ACL to filter SNMP packets.

```
device# configure terminal
device(config)# access-list 25 deny host 10.157.22.98 log
device(config)# access-list 25 deny 10.157.23.0 0.0.0.255 log
device(config)# access-list 25 deny 10.157.24.0 0.0.0.255 log
device(config)# access-list 25 permit any
device(config)# access-list 30 deny 10.157.25.0 0.0.0.255 log
device(config)# access-list 30 deny 10.157.26.0/24 log
device(config)# access-list 30 permit any
device(config)# snmp-server community public ro 25
device(config)# snmp-server community private rw 30
device(config)# write memory
```

The following example associates a view to the members of a community string.

```
device# configure terminal
device(config)# snmp-server community private rw view view1
```

The following example configures a read-only access and a read/write access for the same SNMP community. The output from the **show running-config** command shows that only one access type, the highest access level, is saved in the running configuration.

```
device# configure terminal
device(config)# snmp-server community private ro
device(config)# snmp-server community private rw
device(config)# exit
device# show running-config | inc snmp
snmp-server
snmp-server community private rw
```

History

Release version	Command history
5.9.00	This command was modified to allow setting just one access type for an SNMP community.

snmp-server context

Creates SNMP context and maps the context name to the name of a VPN routing and forwarding (VRF) instance.

Syntax

snmp-server context *context-name* **vrf** *vrf-name*

no snmp-server-context *context-name* **vrf** *vrf-name*

Parameters

context
Enables the specification of a variable *context_name* that can be passed in the SNMP PDU.

context_name
SNMP context name.

vrf
Enables the specification of a variable *vrf_name* that can be retrieved when an SNMP request is sent with the configured *context_name*.

vrf_name
VRF instance name.

Modes

Global configuration mode

Usage Guidelines

The context-to-VRF mapping is one-to-one and is applicable to all SNMP versions.

Examples

The following **snmp-server context** command maps the context name "mycontext" to the VRF name "myvrf".

```
switch(config)# snmp-server context mycontext vrf myvrf
```

The following **snmp-server context** command deletes the SNMP context to VRF map.

```
switch(config)# no snmp-server context mycontext vrf myvrf
```

History

Release version	Command history
05.9.00	This command was introduced.

snmp-server enable mib

Enables MIB support for SNMP server.

Syntax

snmp-server enable mib *snmp-community-mib*

no snmp-server enable mib *snmp-community-mib*

Command Default

MIB support is disabled by default.

Parameters

snmp-community-mib

Enables access for the SNMP community MIBs.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables access for SNMP-COMMUNITY-MIB.

Examples

The following example enables the snmpCommunityTable MIB support.

```
device(config)# snmp-server enable mib snmp-community-mib
```

History

Release version	Command history
05.9.00	This command was introduced.

snmp-server enable traps

Configures error trap generation for IPsec and IKEv2.

Syntax

snmp-server enable traps [**ipsec**] [**ikev2**]

no snmp-server enable traps [**ipsec**] [**ikev2**]

Command Default

By default, IPsec and IKEv2 traps are enabled.

Parameters

ipsec

Configures error trap generation for IPsec.

ikev2

Configures error trap generation for IKEv2.

Modes

Privileged Exec mode

Usage Guidelines

The **no** form of this command disables the generation of IPsec and IKEv2 error traps.

Examples

The following example disables error trap generation for IPsec and IKEv2.

```
device# no snmp-server enable traps ipsec ikev2
```

History

Release version	Command history
5.8.00	This command was introduced.

snmp-server enable traps bum-rl-traps

Configures the SNMP rate-limiting traps for BUM traffic on SNMP servers.

snmp-server enable traps bum-rl-traps

no snmp-server enable traps bum-rl-traps

Command Default

By default, SNMP rate-limiting traps for BUM traffic on SNMP servers are enabled.

Modes

Usage Guidelines

no

Examples

The following example shows how to disable SNMP rate-limiting traps for BUM traffic.

```
device# configure terminal
device(config)# no snmp-server enable traps bum-rl-traps
```

History

Release version	Command history
5.7.00	This command was introduced.

snmp-server host

Configures a trap receiver to ensure that all SNMP traps sent by the Brocade device go to the same SNMP trap receiver or set of receivers, typically one or more host devices on the network.

Syntax

snmp-server host { *host-ipaddr* | **ipv6** *host-ipv6-addr* } [**version** { **v1** | **v2c** } [*community-string* [**port** *port-num*]]]

no snmp-server host { *host-ipaddr* | **ipv6** *host-ipv6-addr* } [**version** { **v1** | **v2c** } [*community-string* [**port** *port-num*]]]

snmp-server host { *host-ipaddr* | **ipv6** *host-ipv6-addr* } [**version v3** { **auth** | **noauth** | **priv** } *name* [**port** *port-num*]]

no snmp-server host { *host-ipaddr* | **ipv6** *host-ipv6-addr* } [**version v3** { **auth** | **noauth** | **priv** } *name* [**port** *port-num*]]

Command Default

The SNMP trap receiver is not configured.

Parameters

host-ipaddr
Specifies the IP address of the trap receiver.

ipv6 *host-ipv6-addr*
Specifies the IPv6 address of the trap receiver.

version
Configures the SNMP version or security model.

v1
Specifies SNMP version 1.

v2c
Specifies SNMP version 2c.

community-string
Specifies an SNMP community string configured on the device.

v3
Specifies SNMP version 3.

auth
Specifies that only authenticated packets with no privacy are allowed to access the specified view. This parameter is available only for SNMPv3 user groups.

noauth
Specifies that no authentication and no privacy are required to access the specified view. This parameter is available only for SNMPv3 user groups.

priv
Specifies that authentication and privacy are required from the users to access the view. This parameter is available only for SNMPv3 user groups.

name

Specifies the SNMP security name or user.

port *port-num*

Configures the UDP port to be used by the trap receiver. The default port number is 162.

Modes

Global configuration mode

Usage Guidelines

The device sends all the SNMP traps to the specified hosts and includes the specified community string. Administrators can therefore filter for traps from a Brocade device based on IP address or community string. When you add a trap receiver, the software automatically encrypts the community string you associate with the receiver when the string is displayed by the CLI or Web Management interface. The software does not encrypt the string in the SNMP traps sent to the receiver.

The SNMP community string configured can be a read-only string or a read-write string. The string is not used to authenticate access to the trap host but is instead a useful method for filtering traps on the host. For example, if you configure each of your Brocade devices that use the trap host to send a different community string, you can easily distinguish among the traps from different devices based on the community strings.

The Multiple SNMP Community Names feature introduced the ability to configure one default community string (where a community string is not mapped to any SNMP context) and one community string per SNMP context for a single trap host. One community name per line is allowed. For protocol-specific MIBS, Brocade devices send the trap originating from specific VRF instance and the corresponding community name mapped to the SNMP context associated with that VRF is sent in the trap. When the Brocade devices send the trap originating from a default VRF instance, the default community string is sent in the trap. Using the community string in the trap, administrators can easily distinguish among the traps originated from different VRF instances. if you enter the **show running-config** command it displays multiple **snmp-server host** command instances for each host; one community name per line.

Specifying the port allows you to configure several trap receivers in a system. With this parameter, a network management application can coexist in the same system. Devices can be configured to send copies of traps to more than one network management application.

The **no** form of the command removes the configured SNMP server host.

Examples

The following example configures 10.10.10.1 as the trap receiver.

```
device(config)# snmp-server host 10.10.10.1 version v2c mypublic port 200
```

The following example configures 2002::2:2 as the trap receiver and specifies that only authenticated packets with no privacy are allowed to access the specified view.

```
device(config)# snmp-server host ipv6 2002::2:2 version v3 auth user-private port 110
```

The following example configures multiple SNMP community names for a single trap host.

```
device(config)# snmp-server host 192.168.2.1 version v1 user-community1
device(config)# snmp-server host 192.168.2.1 version v1 user-community2
device(config)# snmp-server host 192.168.2.1 version v1 user-community3
```

History

Release version	Command history
5.9.00	This command was modified to allow multiple SNMP community names to be configured for a single trap host.

snmp-server mib community-map

Maps an existing SNMP community string with an existing 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-map
: Maps SNMP community string to any routing instance specified in the variable *community-name*.

community_name
: The existing or already configured SNMP community string.

context
: Enables the specification of a variable *context_name* that can be passed in the SNMP PDU.

community_name
: The existing or already configured SNMP context name.

Modes

Global configuration mode

Usage Guidelines

The SNMP community and SNMP context must be configured before mapping.

Examples

The following example enables the snmpCommunityTable MIB support.

```
device(config)# snmp-server mib community-map <community-name>
context <context-name>
```

History

Release version	Command history
05.9.00	This command was introduced.

spanning-tree pvst-protect

Enables or disables Per VLAN Spanning Tree (PVST) protection for all global interfaces running xSTP.

Syntax

spanning-tree pvst-protect do-disable

spanning-tree pvst-protect re-enable [**ethernet** *slot*/*port* [**to** *slot*/*port*]]

no spanning-tree pvst-protect do-disable

no spanning-tree pvst-protect re-enable [**ethernet** *slot*/*port* [**to** *slot*/*port*]

Command Default

By default, PVST protect configuration is independent of spanning tree global configuration.

Parameters

do-disable

Disables the PVST protection globally on VLANs when xSTP is configured and also can coexist with per VLAN xSTP configuration.

re-enable

Re-enables the PVST protect disabled interfaces globally.

ethernet *slot*/*port* **to** *slot*/*port*

Specifies an Ethernet interface or a range of Ethernet interfaces on which PVST protection is re-enabled.

Modes

Global configuration mode

Usage Guidelines

PVST is a Cisco proprietary protocol that allows a Cisco device to have multiple spanning trees. The Cisco device can interoperate with spanning trees on other PVST devices but cannot interoperate with IEEE 802.1Q devices. An IEEE 802.1Q device has all its ports running a single spanning tree. PVST+ is an extension of PVST that allows a Cisco device to also interoperate with devices that are running a single spanning tree (IEEE 802.1Q).

Brocade supports PVST plus (PVST+) by allowing a Brocade device to run multiple spanning trees (MSTP) while also interoperating with IEEE 802.1Q devices. Ports automatically detect PVST+ BPDUs and enable support for the BPDUs once detected. The PVST+ support allows a Brocade device to interoperate with PVST spanning trees and the IEEE 802.1Q spanning tree at the same time.

The **no spanning-tree pvst-protect do-disable** command disables the PVST protect feature configuration globally, and enables all the ports which were disabled by this feature.

The **no spanning-tree pvst-protect re-enable** command reenables the PVST protect feature configuration globally, or for a specific or range of Ethernet interfaces and enables the specified ports.

NOTE
PVST protect configuration is not applicable for an Inter-Chassis Link (ICL) port.

Examples

The following example disables the PVST protect feature configuration globally.

```
device# configure terminal
device(config)# spanning-tree pvst-protect do-disable
```

The following example re-enables the PVST protect feature configuration on Ethernet interfaces 1/5 through 1/7

```
device# configure terminal
device(config)# spanning-tree pvst-protect re-enable ethernet 1/5 to 1/7
```

History

Release version	Command history
5.7.00	This command was introduced.

spf-interval

Changes the shortest path first (SPF) interval.

Syntax

spf-interval [**level-1** | **level-2**] *max-wait* [*initial-wait*] [*second-wait*]

no spf-interval

Parameters

level-1
Specifies Level 1 packets only.

level-2
Specifies Level 2 packets only.

max-wait
Specifies the maximum interval in seconds between SPF recalculations. The range is 0 - 120 seconds. The default is 5 seconds.

initial-wait
Specifies the initial SPF calculation delay in milliseconds after an LSP change. The range is 0 to 120000 milliseconds. The default is 5000 milliseconds (5 seconds).

second-wait
Indicates the hold time between the first and second SPF calculation in milliseconds. The range is 1 to 120000 milliseconds. The default is 5000 milliseconds (5 seconds).

Modes

ISIS router configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example specifies that the maximum interval in seconds between SPF recalculations is 15 seconds. The initial SPF calculation delay is 10000 milliseconds and the hold time between the first and second SPF calculation is 15000 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# spf-interval 15 10000 15000
```

The following example restores the defaults.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no spf-interval
```

The following example specifies that the maximum interval in seconds between SPF recalculations is 15 seconds for level 1 packets. The initial SPF calculation delay is 10000 milliseconds and the hold time between the first and second SPF calculation is 15000 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# spf-interval level-1 15 10000 15000
```

state-name

Configures the state name where the Public Key Infrastructure (PKI) entity resides.

Syntax

state-name *string*

no state-name *string*

Command Default

No state is recorded, by default.

Parameters

string

Specifies the name of the state for PKI entity.

Modes

PKI entity configuration mode

Examples

The following example configures California as the state where the PKI entity named as Brocade-entity resides.

```
device# configure terminal
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# state-name California
```

History

Release version	Command history
5.8.00	This command was introduced.

static-lsp

Creates a new static label-switched path (LSP) at the transit router or enters into the mode of an existing static transit LSP to modify its parameters and enable or disable the static transit LSP.

Syntax

static-lsp transit *name*

no static-lsp transit *name*

Parameters

transit *name*

Configures a new static LSP at a transit router. If the *name* is an existing static transit LSP name, it enters into the configuration mode for that static transit LSP.

Modes

MPLS configuration mode

Usage Guidelines

The LSP name must be unique within that router for static transit LSPs.

Use the **no** option to delete the static LSP.

Examples

The following example configures a static transit LSP named t1.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# static-lsp transit t1
device(config-mpls-static-transit-lsp-t1)# in-label 16
device(config-mpls-static-transit-lsp-t1)# next-hop 3.3.3.3
device(config-mpls-static-transit-lsp-t1)# out-label 17
device(config-mpls-static-transit-lsp-t1)# enable
```

History

Release version	Command history
5.5.00	This command was introduced.

static-mac-address

Configures the static MAC address on the VPLS endpoints.

static-mac-address { *mac-addr* **ethernet** *slot/port* }

no static-mac-address { *mac-addr* **ethernet** *slot/port* }

Parameters

mac_addr
: Identifies the selected MAC address.

ethernet
: Selects the Ethernet MAC address.

slot/port
: Ethernet port of the VPLS endpoint.

Modes

Usage Guidelines

no

Multicast, broadcast, and zero-MACs cannot be configured.

Examples

The following example displays how to configure static MAC address on VPLS endpoints.

```
device(config)# router mpls
device(config-mpls)# vpls vpls-1 1
device(config-mpls-vpls-1)# vlan 900 inner-vlan 800
device(config-mpls-vpls-1-vlan-900)# static-mac-address 0000.1111.3333 ethernet 1/20
```

The following example displays removing a configured static MAC from a tagged/untagged endpoint.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# vpls vpls-1 1
device(config-mpls-vpls-1)# vlan 900
device(config-mpls-vpls-1-vlan-900)# no static-mac-address 0000.1111.2222 ethernet 1/23
```

History

Release version	Command history
5.7.00	This command is introduced.

statistics-load-interval

Configures the load interval parameter for calculating the bit rate and packet count for the access-list accounting statistics.

Syntax

statistics-load-interval { *seconds* | **accumulated** }

no statistics-load-interval { *seconds* | **accumulated** }

Parameters

seconds

Specifies the load interval values. Permitted values are **1**, **60**, or **300**.

accumulated

Displays accumulated ACL statistics packets and bit rate counts.

Modes

ACL-policy sub-configuration mode

Usage Guidelines

The **no** form of the command removes the configuration of the load interval parameters for calculating the bit rate and packet count for the access-list accounting statistics.

Use the configured load interval value to display the bit rate and packet rate statistics. If the load interval is not configured, statistics of all three intervals *1s/60s/300s* and accumulated statistics display.

This configuration is stored in the configuration file.

NOTE
This configuration applies only to policy-based routing ACLs.

Examples

The following example uses the load interval option to choose any one of the intervals for statistics display.

```
device(config)# acl-policy
device(config-acl-policy)# statistics-load-interval 60
device(config-acl-policy)# show access-list accounting brief policy-based-routing
Intf      ACL     BitRate        HitRate
3/1     100     2697753600     2634525(1m)
3/3     101     5210585952     4934267(1m)
3/3     102     0              0(1m)
```

The following example shows uses the non-zero statistics option.

```
device(config)# acl-policy
device(config-acl-policy)#
device(config-acl-policy)# show access-list accounting brief policy-based-routing omit-zero
Intf    ACL     BitRate        HitRate
3/1     100     2697753600     2634525(1m)
3/3     101     5210585952     4934267(1m)
```

History

Release version	Command history
5.8.00	This command was introduced.

strip-802-1br

Use the **strip-802-1br** command to remove the 802.1BR header and forward the packets to the next processing port for further filtering and forwarding.

Syntax

strip-802-1br { **all** | **slot** *slot-num* | **slot** *slot-num* **device-id** *device-id* }

no strip-802-1br { **all** | **slot** *slot-num* | **slot** *slot-num* **device-id** *device-id* }

Command Default

The 802.1BR header is not stripped.

Parameters

all

Configures the functionality on all the ppcrs

slot

Represents the module ID.

device-id

Represents the NP-ID.

Modes

Packet-encap-processing (config-pkt-encap-proc) configuration mode.

Usage Guidelines

The feature can be disabled on all slots (globally) by using the **all** keyword.

The feature can be disabled on selective slots by using the **slot** keyword.

The feature can be disabled on selective PPCRs by using the **slot** and **device** keywords.

This feature is supported on the following modules:

- BR-MLX-40Gx4
- BR-MLX-10Gx20
- BR-MLX-100Gx2-CFP2

For unsupported cards this is a non-operation.

NOTE
Stripping and preservation features can not be configured on same set of ppcrs.

Examples

The following example configures the command on all PPCRs.

```
device(sw)# config terminal
device(config)# packet-encap-processing
device(config-pkt-encap-proc)# strip-802-1br all
```

The following example configures the feature on slot 3 and slot 4 device-id 1.

```
device(sw)# config terminal
device(config)# packet-encap-processing
device(config-pkt-encap-proc)# strip-802-1br slot 3
device(config-pkt-encap-proc)# strip-802-1br slot 4 device-id 1
```

History

Release version	Command history
6.0.00a	This command was introduced.

strip-vn-tag

Use the **strip-vn-tag** command to remove the VN-tag header and forward the packets to the next processing port for further filtering and forwarding.

Syntax

strip-vn-tag { **all** | **slot** *slot-num* | **slot** *slot-num* **device-id** *device-id* }

no strip-vn-tag { **all** | **slot** *slot-num* | **slot** *slot-num* **device-id** *device-id* }

Command Default

The VN-tag header is not stripped.

Parameters

all

Configures the functionality on all the ppcrs

slot

Represents the module ID.

device-id

Represents the NP-ID.

Modes

Packet-encap-processing (config-pkt-encap-proc) configuration mode.

Usage Guidelines

The feature can be disabled on all slots (globally) by using the **all** keyword.

The feature can be disabled on selective slots by using the **slot** keyword.

The feature can be disabled on selective PPCRs by using the **slot** and **device** keywords.

This feature is supported on the following modules:

- BR-MLX-40Gx4
- BR-MLX-10Gx20
- BR-MLX-100Gx2-CFP2

For unsupported cards this is a non-operation.

NOTE
Stripping and preservation features can not be configured on same set of ppcrs.

Examples

The following example configures the feature on all PPCRs.

```
device(sw)# config terminal
device(config)# packet-encap-processing
device(config-pkt-encap-proc)# strip-vn-tag all
```

The following example configures the feature on slot 3 and slot 4 device-id 1.

```
device(sw)# config terminal
device(config)# packet-encap-processing
device(config-pkt-encap-proc)# strip-vn-tag slot 3
device(config-pkt-encap-proc)# strip-vn-tag slot 4 device-id 1
```

History

Release version	Command history
6.0.00a	This command was introduced.

subject-alt-name

Configures the alternative subject name for the Public Key Infrastructure (PKI) entity.

Syntax

subject-alt-name *string*

no subject-alt-name *string*

Parameters

string

Specifies the alternate name of the subject for the PKI entity. The supported attributes are email address, DNS, IP address, URI, dirname and router ID (RID).

Modes

PKI entity configuration mode

Usage Guidelines

If the IKE peer uses an ID other than the distinguished name (DN), then that should be mentioned in the **subject-alt-name**. If the certificate does not have subject-alt-name then use DN for the IKE ID.

Examples

The following example shows how to configure an alternate name of the subject for the PKI entity.

```
device(config)# pki entity brocade
device(config-pki-entity-brocade)# subject-alt-name red
```

The following example shows how to configure an alternate name of the subject for the PKI entity, by specifying an email address and URI.

```
device(config)# pki entity brocade
device(config-pki-entity-brocade)# email:my@other.address,URI:http://my.url.here/
```

The following example shows how to configure an alternate name of the subject for the PKI entity, by specifying an IP address.

```
device(config)# pki entity brocade
device(config-pki-entity-brocade)# IP:192.168.7.1
```

The following example shows how to configure an alternate name of the subject for the PKI entity, by specifying an email address and router ID.

```
device(config)# pki entity brocade
device(config-pki-entity-brocade)# email:my@other.address,RID:1.2.3.4
```

History

Release version	Command history
05.8.00	This command was introduced.
06.0.00a	Modified to include additional configuration examples.

summary-address

Configures route summarization to aggregate IS-IS route information.

Syntax

summary-address *ip-address subnet-mask* [**level-1** | **level-1-2** | **level-2**]

nosummary-address *ip-address subnet-mask* [**level-1** | **level-1-2** | **level-2**]

Command Default

Disabled.

Parameters

ip-address

Specifies an IP address.

subnet-mask

Specifies a subnet mask.

level-1

Specifies that only routes redistributed into Level 1 are summarized with the configured address and mask value.

level-1-2

Specifies that routes redistributed into Level 1 and Level 2are summarized with the configured address and mask value.

level-2

Specifies that only routes redistributed into Level 2 are summarized with the configured address and mask value.

Modes

ISIS address-family IPv4 unicast configuration mode

Usage Guidelines

When you configure a summary address, the address applies only to Level-2 routes by default.

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 10.2.2.2 for Level 1 and Level 2 routes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-isis-router-ipv4u)# summary-address 10.1.0.0 10.2.2.2 level-1-2
```

summary-address (OSPFv2)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address *A.B.C.D E.F.G.H*

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A.B.C.D E.F.G.H

IP address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.This parameter affects only imported, type 5 external routes.

The no form of the command disables route summarization.

Examples

The following example configures a summary address of 10.1.0.0 with a mask of 10.255.0.0:

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# summary-address 10.1.0.0 10.255.0.0
```

NOTE

The command in this example configures summary address 10.1.0.0, which 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.

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 32 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.

If you use redistribution filters in addition to address ranges, the Brocade device applies the redistribution filters to routes first, then applies them to the address ranges.

If you disable redistribution, all the aggregate routes are flushed, along with other imported routes.

This option affects only imported, type 5 external routes. A single type 5 LSA is generated and flooded throughout the AS for multiple external routes.

Examples

The following example configures a summary address of 2001:db8::/24 for routes redistributed into OSPFv3.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# summary-address 2001:db8::/24
```

NOTE

In this example, 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.

summary-prefix

Configure summary prefixes to aggregate IPv6 IS-IS route information.

Syntax

summary-prefix *ipv6-prefix prefix-length* [**level-1** | **level-1-2** | **level-2**]

no summary-prefix *ipv6-prefix prefix-length* [**level-1** | **level-1-2** | **level-2**]

Command Default

Disabled.

Parameters

ipv6-prefix prefix-length

Specifies the aggregate address. You must specify the ipv6-prefix parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. You must specify the prefix-length parameter as a decimal value. A slash mark (/) must follow the ipv6-prefix parameter and precede the prefix-length parameter.

level-1

Specifies that only routes redistributed into Level 1 are summarized

level-1-2

Specifies that routes redistributed into Level 1 and Level 2 are summarized

level-2

Specifies that only routes redistributed into Level 2 are summarized.

Modes

ISIS address-family IPv6 unicast configuration mode

Usage Guidelines

When you configure a summary address, the address applies only to Level-2 routes by default.

The **no** form of the command disables route summarization.

Examples

The following example configures a summary prefix of 2001:db8::/32 to be advertised to Level-1 routes only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-prefix 2001:db8::/32 level-1
```

suppress-acl-seq

Hides or suppresses the display and storage of sequence numbers for ACL entries.

Syntax

suppress-acl-seq

no suppress-acl-seq

Modes

acl-policy configuration mode

Usage Guidelines

Use this command if you need to downgrade a device to an earlier version of software that does not support ACL entry sequence numbers, you should configure **suppress-acl-seq** prior to the downgrade. Otherwise, ACL configurations created with the **suppress-acl-seq** parameter will result in an error on previous releases.

The **no** version of this command resets the configuration to display sequence numbers.

Examples

The following example suppresses ACL entry sequence numbering:

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# suppress-acl-seq
```

History

Release	Command History
5.6.00	This command was introduced.

suppress-ipv6-priority-mapping

Suppresses the IPv6-priority-mapping command from IPv6 filters. This command is only to be used before starting the downgrade process.

Syntax

suppress-ipv6-priority-mapping

Modes

acl-policy

Usage Guidelines

Use this command if you need to downgrade a device to an earlier version of software that does not support ACL ipv6-priority-mapping, you should configure **suppress-ipv6-priority-mapping** prior to the downgrade. Otherwise, ACL configurations created with the **ipv6-priority-mapping** parameter will result in an error on previous releases.

To reset the **ipv6-priority-mapping**, re-appy the command using the **ipv6-access-list**.

Examples

The following example suppresses ACL IPv6 priority-mapping.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# suppress-ipv6-priority-mapping
```

History

Release version	Command history
6.0.0	This command was introduced.

sysmon fe link auto-tune

Enables auto tuning on the fabric element (FE).

Syntax

sysmon fe link auto-tune

no sysmon fe link auto-tune

Command Default

Auto tuning on the FE is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables auto-tuning on the FE.

Examples

The following example disables auto-tuning on the FE.

```
device(config)# no sysmon fe link auto-tune
```

History

Release version	Command history
05.6.00	This command was introduced.

sysmon ipc rel-q-mon enable

Enables LP and MP IPC reliable transmission (TX) queue monitoring and the generation of syslog messages when the IPC reliable TX queue is stuck or recovers from being stuck.

Syntax

sysmon ipc rel-q-mon enable

no sysmon ipc rel-q-mon enable

Command Default

IPC reliable TX queue monitoring is disabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables LP and MP IPC reliable transmission (TX) queue monitoring.

Examples

The following example enables IPC reliable TX queue monitoring and syslog message generation.

```
device(config)# sysmon ipc rel-q-mon enable
```

The following example disables IPC reliable TX queue monitoring and syslog message generation.

```
device(config)# no sysmon ipc rel-q-mon enable
```

History

Release version	Command history
6.0.00	This command was introduced.

sysmon lp-high-cpu enable

Configures high cpu-usage and reporting on interface modules.

Syntax

sysmon lp-high-cpu enable [**all** | *slot-number*]

no sysmon lp-high-cpu enable [**all** | *slot-number*]

Parameters

all

Specifies CPUs on all slots to be monitored.

slot-number

Specifies the slot number for the CPU to be monitored.

Modes

Privileged EXEC configuration mode.

Usage Guidelines

Use this command to set up the monitoring on one or all LP CPUs.

The **no** form of this command disables the LP CPU high-usage monitoring.

Examples

The following example enables monitoring on all CPUs.

```
device(config)# sysmon lp-high-cpu enable all
```

The following example enables monitoring on the CPU in slot 7.

```
device(config)# sysmon lp-high-cpu enable 7
```

History

Release	Command History
05.9.00	This command was introduced.

sysmon lp-high-cpu threshold

Configures high cpu-usage and reporting on interface modules.

Syntax

sysmon lp-high-cpu threshold *decimal-percent-number*

no sysmon lp-high-cpu threshold

Parameters

decimal-percent-number

Specifies the usage threshold for all CPUs to be monitored. Acceptable range of values is from 50 to 100 with 80 as the default value.

Modes

Privileged EXEC configuration mode.

Usage Guidelines

Use this command to set up the usage threshold for collecting data on the monitored LP CPUs. The default CPU threshold is 80% unless explicitly specified. The set threshold applies to all LP(s).

The **no** form of this command resets the usage threshold to 80% for all CPUs.

Examples

The following example sets the usage threshold to 90% for all monitored CPUs.

```
device(config)# sysmon lp-high-cpu threshold 90
```

The following resets the usage threshold to 80% for all monitored CPUs.

```
device(config)# no sysmon lp-high-cpu threshold
```

History

Release	Command History
05.9.00	This command was introduced.

sysmon mp-high-cpu cpu-threshold

Configures the MP CPU usage threshold that triggers data collection into a log file.

Syntax

sysmon mp-high-cpu cpu-threshold *decimal-cpu-percentage*

no sysmon mp-high-cpu cpu-threshold

Command Default

When high CPU monitoring on the MP is enabled, the default CPU usage threshold is 90 percent.

Parameters

decimal-cpu-percentage

Specifies the threshold based on the percentage of usage on the monitored MP CPUs. The percentage values are from 60 through 100. The default percentage value is 90.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the usage threshold for collecting data on the monitored active and standby MP CPUs when MP CPU high-usage monitoring is enabled.

The threshold is based on the percentage of CPU usage on the active or standby MP.

The **no** form of the command resets the usage threshold to the default value of 90 percent for the MP CPUs.

Examples

The following command example sets the usage threshold to 70 percent for the MP CPUs.

```
device(config)# sysmon mp-high-cpu cpu-threshold 70
```

The following command example resets the usage threshold to 90 percent for the MP CPUs.

```
device(config)# no sysmon mp-high-cpu cpu-threshold
```

History

Release version	Command history
6.0.00	This command was introduced.

sysmon mp-high-cpu enable

Enables MP CPU high-usage monitoring and data collection in a log file.

Syntax

sysmon mp-high-cpu enable

no sysmon mp-high-cpu enable

Command Default

MP CPU high-usage monitoring is disabled.

Modes

Global configuration mode

Usage Guidelines

Use this command to enable CPU high-usage monitoring on the active and standby MP CPUs and log high CPU usage events in a log file. Monitoring is enabled when the MP is in the up state.

The **no** form of the command disables MP CPU high-usage monitoring and data collection. Also, the threshold settings that were configured when monitoring was enabled are reset to their default values of 90 percent and 400 ms.

Examples

The following example enables MP CPU high-usage monitoring and data collection.

```
device(config)# sysmon mp-high-cpu enable
```

The following example disables MP CPU high-usage monitoring and data collection. Also, the threshold settings are reset to their default values.

```
device(config)# no sysmon mp-high-cpu enable
```

History

Release version	Command history
6.0.00	This command was introduced.

sysmon mp-high-cpu task-threshold

Configures the MP CPU task threshold that triggers data collection in a log file.

Syntax

sysmon mp-high-cpu task-threshold *ms*

no sysmon mp-high-cpu task-threshold

Command Default

When high CPU monitoring on the MP is enabled, the default task threshold is 400 milliseconds (ms).

Parameters

ms

Specifies the threshold based on the time in milliseconds that the task holds the MP CPU. The millisecond values are from 100 through 500. The default threshold is 400.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the task threshold for collecting data on the monitored active and standby MP CPUs when MP CPU high-usage monitoring is enabled.

The threshold is the amount of time that the task holds the MP CPU.

The **no** form of the command resets the task threshold to the default value of 400 ms.

Examples

The following example sets the task threshold to 200 ms.

```
device(config)# sysmon mp-high-cpu task-threshold 200
```

The following example resets the task threshold to 400 ms.

```
device(config)# no sysmon mp-high-cpu task-threshold
```

History

Release version	Command history
6.0.00	This command was introduced.

sysmon np memory-errors

Configures memory error monitoring and reporting on interface modules.

Syntax

sysmon np memory-errors [**action** { **none** | **syslog** | **syslog-and-trap** | **trap** }]

sysmon np memory-errors [**polling-period** *secs*]

sysmon np memory-errors [**schedule** { **after** *dd:hh:mm* | **at** *hh:mm:ss mm-dd-yy* | **now** } *runs*]

sysmon np memory-errors [**slot** { **all** | *slot* }]

no sysmon np memory-errors [**action** { **none** | **syslog** | **syslog-and-trap** | **trap** }]

no sysmon np memory-errors [**polling-period** *secs*]

no sysmon np memory-errors [**schedule** { **after** *dd:hh:mm* | **at** *hh:mm:ss mm-dd-yy* | **now** } *runs*]

no sysmon np memory-errors [**slot** { **all** | *slot* }]

Parameters

action

Specifies the action taken when NP memory errors are detected. The default action is syslog-and-trap.

none

No action; reporting of errors is disabled. In the no form of the command, specifying the action as none restores the default action (syslog-and-trap).

syslog

Generates a syslog message.

syslog-and-trap

Generates a syslog message and a SNMP trap.

trap

Sends a SNMP trap.

polling-period *secs*

Specifies the frequency of polling for NP memory errors. The range is from 1 through 65535. The default value is 60 seconds.

schedule

Configures the test scheduling.

after *dd:hh:mm*

Specifies that the test is run after the specified amount of time.

at *hh:mm:ss mm-dd-yy*

Specifies that the test is run at the specified time and date.

now

Specifies that the test is run immediately. This is defined as on-demand testing.

runs

Specifies the number of test runs.

slot

Specifies the slots on which the test is run.

all

Specifies that the test is run on all slots.

slot

Specifies the slot number on which the test is to be run. You can specify up to 8 slot numbers.

Modes

Global configuration mode

Usage Guidelines

The **action** parameter controls the generation of syslog messages or SNMP traps. These messages cannot be controlled by the **no snmp-server enable traps** command or the **no logging enable** command. If the **action** option is configured as **syslog** followed by a configuration of the **trap** action, the action becomes **syslog-and-trap**.

The **polling-period** parameter determines the interval between checks for NP memory errors. Reporting may not happen within the polling interval; it may be delayed by factors such as a high CPU load on either the interface or management modules, low memory, or other factors.

Memory errors are detected on the interface module. Errors may not be reported if there is a communication problem between the management module and the interface module.

The **no** form of this command disables memory error monitoring on interface modules.

Examples

The following example specifies polling for NP memory errors at 10 second intervals.

```
device# configure terminal
device(config)# sysmon np memory-errors polling-period 10
```

The following example disables reporting of NP memory errors.

```
device# configure terminal
device(config)# sysmon np memory-errors action none
```

The following example disables monitoring of memory errors on interface modules.

```
device# configure terminal
device(config)# no sysmon np memory-errors
```

The **no** form of the command specifying a **polling-period** value restores the default polling interval. For example, the following example restores the polling interval to the default value of 60 seconds.

```
device# configure terminal
device(config)# no sysmon np memory-errors polling-period 1000
```

The following example removes the **syslog** action.

```
device# configure terminal
device(config)# no sysmon np memory-errors action syslog
```

The following example restores the default action of **syslog-and-trap**. The **no** form of the command specifying the **action none** parameters restores the default action.

```
device# configure terminal
device(config)# no sysmon np memory-errors action none
```

History

Release	Command History
5.6.00	This command was introduced.

sysmon port port-crc-test

Enables the port CRC error monitoring test.

Syntax

sysmon port port-crc-test [**action** {**none** | **port-disable** | **syslog** }]

sysmon port port-crc-test [**counter port-crc-counter less-than** *crc-count*]

sysmon port port-crc-test [**log-backoff** *num*]

sysmon port port-crc-test [**polling-period** *seconds*]

sysmon port port-crc-test [**schedule** { **after***dd:hh:mm runs* | **at** *hh:mm:ss mm-dd-yy runs* | **now** }]

sysmon port port-crc-test [**slot** { **all** | *slot* }]

sysmon port port-crc-test [**threshold** *num-failures num-polls*]

no sysmon port port-crc-test [**action** {**none** | **port-disable** | **syslog** }]

no sysmon port port-crc-test [**counter port-crc-counter less-than** *crc-count*]

no sysmon port port-crc-test [**log-backoff** *num*]

no sysmon port port-crc-test [**polling-period** *seconds*]

no sysmon port port-crc-test [**schedule** { **after***dd:hh:mm runs* | **at** *hh:mm:ss mm-dd-yy runs* | **now** }]

no sysmon port port-crc-test [**slot** { **all** | *slot* }]

no sysmon port port-crc-test [**threshold** *num-failures num-polls*]

Parameters

action

Specifies a sysmon action configuration.

none

No action.

port-disable

Disable port.

syslog

Generates a syslog message.

counter port-crc-counter less-than *crc-count*

Specifies the port CRC error count limit for the configured polling period. The range of values is 0 through 65535. The default value is 20.

polling-period *secs*

Specifies the polling period in seconds. The range of values is 0 through 65535. The default value is 60 seconds.

schedule

Specifies the schedule of the test.

after *dd:hh:mm runs*

Specifies that the test is run after the specified amount of time and for the number of test runs.

at *hh:mm:ss mm-dd-yy runs*
Specifies that the test is run at the specified time and date and for the number of test runs.

now
Specifies that the test is run immediately. This is defined as on-demand testing.

slot
Specifies the slots on which the test is run.

all
Specifies that the test is run on all slots.

slot
Specifies the slot number on which the test is to be run. You can specify up to 8 slot numbers.

threshold
Specifies the threshold of the diagnostic test.

num-failures
Specifies the number of failed test runs. The range of values is 1 through 31.

num-polls
Specifies the number of polls (tests). The range of values is 2 through 31.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables the port CRC error monitoring test.

Examples

The following example disables the port CRC error monitoring test.

```
device(config)# no sysmon port port-crc-test
```

The following example sets the diagnostic action to disable the port when the port CRC error limit crosses the configured threshold.

```
device(config)# sysmon port port-crc-test action port-disable
```

The following example configures the port CRC error counter limit to 20.

```
device(config)# sysmon port port-crc-test counter port-crc-counter less-than 20
```

History

Release	Command History
5.5.00	This command was introduced.

sysmon sfm walk auto

Enables an option that automatically triggers a high-speed Switch Fabric Module (hSFM) walk automatically upon reaching a configured threshold.

Syntax

sysmon sfm walk auto

no sysmon sfm walk auto

Command Default

The command is disabled by default.

Modes

Global configuration mode

Usage Guidelines

NOTE
Auto-tuning and hSFM auto-walk cannot operate at the same time. To avoid conflict, configure auto-tuning and hSFM auto-walk to trigger consecutively. Whichever triggers first runs, after which the other one runs.

The **no** form of this command disables the automatic triggering of **sysmon sfm walk auto**.

Examples

The following example enables **sysmon sfm walk auto**.

```
device# configure terminal
device(config)# sysmon sfm walk auto
```

History

Release version	Command history
5.7.00b	This command is introduced.

sysmon sfm walk polling-period

Configuring a polling period for re-assembly errors located on a high-speed Switch Fabric Module (hSFM).

Syntax

sysmon sfm walk polling-period *value*

Command Default

The command is disabled by default.

Parameters

value

Sets the polling period in a range from 1 to 600 seconds. The default setting is 30 seconds.

Modes

Global configuration mode

Usage Guidelines

Use this command to set the interval between polling periods for re-assembly errors.

Examples

The following example configures the sfm walk polling-period to be 50 seconds.

```
device# configure terminal
device(config)# sysmon sfm walk polling-period 50
```

History

Release version	Command history
5.7.00b	This command was introduced.

sysmon sfm walk redundancy-check

Setting an option to automatically trigger an SFM redundancy check during a high-speed Switch Fabric Module (hSFM) walk.

Syntax

sysmon sfm walk redundancy-check

no sysmon sfm walk redundancy-check

Command Default

The redundancy check option is enabled.

Modes

Global configuration mode

Usage Guidelines

For an SFM walk to begin, a redundant SFM is required. The no form of this command will trigger auto hsfm walk if N+1 SFMs are unavailable.

Examples

The following example enables a **sysmon sfm walk redundancy-check**.

```
device# configure terminal
device(config)# sysmon sfm walk redundancy-check
```

History

Release version	Command history
5.7.00b	This command is introduced.

sysmon sfm walk start

Enables a manual high-speed Switch Fabric Module (hSFM) walk.

Syntax

sysmon sfm walk start

Command Default

By default, sysmon sfm walks are automatically triggered.

Modes

Global configuration mode.

Usage Guidelines

Use this command to manually start a sysmon sfm walk.

NOTE
Auto-tuning and hSFM walk cannot operate at the same time. To avoid conflict, auto-tuning and hSFM walk will be performed consecutively. Whichever is triggered first will run and then the other will be performed.

Examples

The following example manually enables sysmon sfm walk.

```
device# configure terminal
device(config)# sysmon sfm walk start
```

History

Release version	Command history
5.7.00b	This command was introduced.

sysmon sfm walk status

Displays the status of a high-speed Switch Fabric Module (hSFM) walk.

Syntax

sysmon sfm walk status

Command Default

This command will show the status of the current SFM walk. If the **auto sfm walk** is disabled, the status of the last walk will be displayed.

Modes

Global configuration mode.

Usage Guidelines

The command is used to display the current status of an active sfm walk or sfm auto-walk.

Examples

The following example enables **sysmon sfm walk status**.

```
device# configure terminal
device(config)# sysmon sfm walk status

=====================================================================
SFM Walk status             : Isolated an SFM
Number of SFM walk done     : 1
Auto walk                   : Enabled
Manual walk                 : Not started
Autotune in progress        : 0
Autotunes on isolated SFM   : 0
AutoWalk timers             :
    Threshold for re-assembly 1, polling period 30, Counter reset time 10000
Redundancy check            : Enable
AutoWalk result             :
    Isolated SFM 3, Current SFM 3 (SFM range (1-4), FE (1-3))
Re-assembly error count 0, MCAST FID updates 0
Reachability register (0x461) dump  :
SFM1/FE1: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM1/FE2: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM1/FE3: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM2/FE1: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM2/FE2: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM2/FE3: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM3/FE1: val=0x01f3f000 : 00000001-11110011-11110000-00000000b [Non-reachable, autotune 0]
SFM3/FE2: val=0x01f3f000 : 00000001-11110011-11110000-00000000b [Non-reachable, autotune 0]
SFM3/FE3: val=0x01f3f000 : 00000001-11110011-11110000-00000000b [Non-reachable, autotune 0]
SFM4/FE1: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM4/FE2: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
SFM4/FE3: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
=====================================================================
```

History

Release version	Command history
05.7.00b	This command was introduced.

sysmon sfm walk stop

Stops any currently running high-speed Switch Fabric Module (hSFM) walk.

Syntax

sysmon sfm walk stop

Command Default

Existing fsm walks run until completed.

Modes

Global configuration mode

Usage Guidelines

This command is used to stop a currently running walk or revert an already completed walk. For example, if an SFM walk is completed and an SFM is isolated, **sysmon sfm walk stop** will re-enable the isolated SFM. This command is effective on both manual and auto SFM walks.

Examples

The following example stops an active sysmon sfm walk.

```
device# configure terminal
device(config)# sysmon sfm walk stop
```

History

Release version	Command history
5.7.00b	This command was introduced.

sysmon sfm walk threshold

Configures the threshold value for a minimum re-assembly count to isolate an SFM during an SFM walk.

Syntax

sysmon sfm walk threshold *value*

no sysmon sfm walk threshold

Command Default

The default sysmon sfm walk threshold value is 1.

Parameters

value

Configures the minimum threshold value for re-assembly count range in a range from 1 to 65535. The default setting is 1.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command will reset the threshold value to the default.

Examples

The following example configures the **sysmon sfm walk threshold** to 5.

```
device# configure terminal
device(config)# sysmon sfm walk threshold 5
```

The following is an example of the syslog showing the resulting actions when re-assembly errors cross the configured threshold value of 5.

```
SYSLOG: <9>Oct 14 00:41:18 System: Health Monitoring: TM Egress data errors detected on LP 15/TM 1
SYSLOG: <14>Oct 14 00:41:18 System: SFM-WALK: Auto SFM walk started
SYSLOG: <14>Oct 14 00:41:18 System: SFM-WALK: Disabling SFM #1
SYSLOG: <9>Oct 14 00:41:32 System: Health Monitoring detects an issue on egress LP 3/TM 1
SYSLOG: <14>Oct 14 00:41:32 System: SFM-WALK: Auto SFM walk started
SYSLOG: <14>Oct 14 00:41:32 System: SFM-WALK: SFM walk in progress
SYSLOG: <9>Oct 14 00:41:46 System: Health Monitoring detects an issue on egress LP 1/TM 1
SYSLOG: <14>Oct 14 00:41:46 System: SFM-WALK: Auto SFM walk started
SYSLOG: <14>Oct 14 00:41:46 System: SFM-WALK: SFM walk in progress
SYSLOG: <9>Oct 14 00:41:48 System: Health Monitoring detects an issue on egress LP 2/TM 2
SYSLOG: <14>Oct 14 00:41:48 System: SFM-WALK: Auto SFM walk started
SYSLOG: <14>Oct 14 00:41:48 System: SFM-WALK: SFM walk in progress
SYSLOG: <14>Oct 14 00:42:01 System: SFM-WALK: Re-assembly errors (125) more than threshold (5). Move to
next SFM #2.
SYSLOG: <14>Oct 14 00:42:42 System: SFM-WALK: Re-assembly errors (126) more than threshold (5). Move to
next SFM #3.
SYSLOG: <14>Oct 14 00:43:22 System: SFM-WALK: Re-assembly errors (0) less than threshold (5). Isolated
SFM #3.
SYSLOG: <14>Oct 14 00:43:22 System: SFM-WALK: SFM walk completed. Faulted SFM #3 and removed from
service.
```

History

Release version	Command history
5.7.00b	This command was introduced.

sysmon tm link auto-tune

Enables auto tuning on the traffic manager (TM).

Syntax

sysmon tm link auto-tune

no sysmon tm link auto-tune

Command Default

Auto tuning on the TM is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables auto-tuning on the TM.

Examples

The following example disables auto-tuning on the TM.

```
device(config)# no sysmon tm link auto-tune
```

History

Release version	Command history
05.6.00	This command was introduced.

system np control-ram-threshold

Configures the CSRAM error reporting threshold parameter for low level memory events.

Syntax

system np control-ram-threshold *threshold*

no system np control-ram-threshold *threshold*

Command Default

The default threshold value is 10.

Parameters

threshold

Specifies the configurable threshold range when low level memory events are exceeded. The decimal range is from 0 - 120 events. The default value is 10.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the CSRAM threshold parameter when monitoring low level memory events occurring with the internal data path of the network processor. This command is enabled by default. Use the **no** form of the command to reset the threshold value to default. Use the command to disable the monitoring of low level memory events. A syslog message and a trap is generated when the CSRAM error events recorded in the rolling window exceeds the configured threshold parameter for the specified port range.

NOTE

Configuring the CSRAM error reporting threshold parameter is supported only on the Brocade NetIron CER Series and the Brocade NetIron CES Series platforms.

Examples

The following example configures the CSRAM error reporting threshold parameter to 20 events.

```
device# configure terminal
device(config)#system np control-ram-threshold 20
```

Use the **show run** command to display the CSRAM error reporting threshold parameter to 20 events.

```
device(config)#show run
!
ver V5.7.0Txxx
!
!
!
no spanning-tree
!
!
vlan 1 name DEFAULT-VLAN
!
!
!
!
system np control-ram-threshold 20
!
!
!
!
!
!
!
!
!
!
end
```

History

Release version	Command history
05.7.00	This command was introduced.

system np lpm-ram-threshold

Configures the LPM memory error reporting threshold parameter for low level memory events.

Syntax

system np lpm-ram-threshold *threshold*

no system np lpm-ram-threshold *threshold*

Command Default

Configuring the LPM memory error reporting threshold parameters is enabled by default.

Parameters

threshold

Specifies the configurable threshold range when low level memory events are exceeded. The decimal range is from 0 - 120 events. The default value is 10.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the LPM memory threshold parameter when monitoring low level memory events occurring with the internal data path of the network processor. The command is enabled by default. Use the **no** form of the command to reset the threshold value to default. Use this command to disable the monitoring of low level memory events. A syslog message and a trap is generated when the LPM memory error events recorded in the rolling window exceeds the configured threshold parameter for the specified port range.

NOTE

Configuring the LPM memory error reporting threshold parameter is supported only on the Brocade NetIron CER Series and the Brocade NetIron CES Series platforms.

Examples

The following example configures the LPM memory error reporting threshold parameter to 20 events.

```
device# configure terminal
device(config)# system np lpm-ram-threshold 20
```

Use the **show run** command to display the LPM memory error reporting threshold parameter to 20 events.

```
device(config)#show run
!
ver V5.7.0Txxx
!
!
!
!
!
no spanning-tree
!
!
vlan 1 name DEFAULT-VLAN
!
!
!
!
!
!
!
!
system np lpm-ram-threshold 20
!
!
!
!
!
!
!
!
!
!
end
```

History

Release version	Command history
5.7.00	This command was introduced.

system-init

Sets system initialization value. A reload is required before this command takes effect.

Syntax

system-init block-g1-sfm

system-init fabric-data-mode { **force-normal** | **force-turbo** }

system-init fabric-failure-detection

system-init fe-access-recovery-disable

system-init max-tm-queues *num*

system-init mlxe32-24x10g-enable [**max-tm-queue-4**]

system-init tm-credit-size { **credit_1024b** | **credit_256b** }

no system-init block-g1-sfm

no system-init fabric-data-mode { **force-normal** | **force-turbo** }

no system-init fabric-failure-detection

no system-init fe-access-recovery-disable

no system-init max-tm-queues *num*

no system-init mlxe32-24x10g-enable [**max-tm-queue-4**]

no system-init tm-credit-size { **credit_1024b** | **credit_256b** }

Parameters

block-g1-sfm

Configures the system to block the g1 switch fabric module.

fabric-data-mode

Configures the fabric data mode.

force-normal

Forces the fabric to use normal data mode.

force-turbo

Forces the fabric to use turbo data mode.

fabric-failure-detection

Configures the system to automatically detect and shutdown the failure fabric.

fe-access-recovery-disable

Disables a RAS feature that will power-cycle switch fabric module if SW cannot access fabric element.

max-tm-queues *num*

Configures the maximum number of queues in the traffic manager to 4.

mlxe32-24x10g-enable

Configures the system to accept 24x10G module.

max-tm-queue-4
Configures the 4-priority mode to allow the coexistance of 24x10G and 2x10, 4x10, and 20x1 modules.

tm-credit-size
Configures the traffic manager credit size.

credit_1024b
Specifies a credit size of 1024 bytes.

credit_256b
Specifies a credit size of 256 bytes.

Modes

Global configuration mode

Usage Guidelines

When using the **fe-access-recovery-disable** option, note that the system does periodic monitoring of FE access and keeps a log for this by code monitoring fabric links and kicks off when number of links down exceeds defined threshold for traffic. However if failure detection configuration is enabled, you need to use these commands for recovery.

Examples

```
device# configure terminal
device(config)#system-init fe-access-recovery-disable
device(config)#exit
device# reload
```

History

Release version	Command history
5.7.00a	This command was introduced.

system-max ecmp-pram-block-size

Configures the maximum parameter random-access memory (PRAM) block allocation for Equal-Cost MultiPath (ECMP) routes.

Syntax

system-max ecmp-pram-block-size *num*

no system-max ecmp-pram-block-size *num*

Parameters

num

Specifies the maximum PRAM block-size value. Valid values are 8, 16, and 32 (default is 32).

Modes

Global configuration mode

Usage Guidelines

The control plane (through the IP load-sharing command) supports up to 32 next hops per route. The actual number of next hops which are programmed in hardware is controlled by this command. When configuring the command to a value lesser than the value configured for IP load-sharing or IPv6 load-sharing, a warning message displays and the value is accepted. When configuring IP load-sharing or IPv6 load-sharing to a value greater than that configured for the command, a warning message displays and the value is accepted.

This command is not supported on Brocade NetIron CER Series and Brocade NetIron CES Series devices.

NOTE
Using this command requires a system restart in order for the new setting to take effect.

Examples

The following example sets the maximum PRAM block-size value to 16.

```
device# configure terminal
device(config)# system-max ecmp-pram-block-size 16
Reload required. Please write memory and then reload or power cycle the system.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.
```

History

Release	Command history
5.5.00	This command was introduced.

system-max ip-arp

Sets the ARP scaling number.

Syntax

system-max ip-arp *num*

Parameters

num

Value range is 2048 - 131072. The default value is 8192.

Modes

Global configuration mode

Usage Guidelines

Use this command to set the maximum number of ARP entries. This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured **system-max** command does not take effect during a hitless-reload.

Examples

The following example sets the maximum number of ARP entries at 3005.

```
device# configure terminal
device(config)# system-max ip-arp 3005
Reload required. Please write memory and then reload or power cycle the system.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.
```

History

Release version	Command history
5.8.00	This command was modified to scale up to 128K ARP entries.

system-max ipv6-receive-cam

Configures the number of IPv6 rACL entries in CAM. The **no** form of this command removes the configured limit and restores the default value.

Syntax

system-max ipv6-receive-cam *num*

no system-max ipv6-receive-cam *num*

Parameters

num

Configures the number of IPv6 rACL entries in CAM. The valid range is from 0 through 8192. The default value is 0.

Modes

Global configuration mode

Usage Guidelines

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured **system-max** command does not take effect during a hitless-reload.

Examples

The following example sets the number of IPv6 rACL entries in CAM to 4096.

```
device# configure terminal
device(config)# system-max ipv6-receive-cam 4096
Reload required. Please write memory and then reload or power cycle the system.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.
```

History

Release version	Command History
5.6.00	This command was introduced.

system-max ipv6-vrf-route

Configures the maximum number of IPv6 routes that can be created per VRF instance.

Syntax

system-max ipv6-vrf-route *num*

no system-max ipv6-vrf-route *num*

Command Default

By default, the maximum number of IPv6 routes per VRF instance is not configured.

Parameters

num

The number of IPv6 routes that can be created per VRF instance. Valid IPv6 route values are 1024 through 131072. The default value is 8192.

Modes

Global configuration mode.

Usage Guidelines

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured **system-max** command does not take effect during a hitless-reload.

Use the **no** form of the command to reset the maximum number of IPv6 routes that was configured for a VRF instance.

Examples

The following example configures 4000 IPv6 routes per VRF instance.

```
device# configure terminal
device(config)# system-max ipv6-vrf-route 4000
```

History

Release version	Command history
5.8.00	This command was modified.

system-max ip-vrf-route

Configures the maximum number of IPv4 routes that can be created per VRF instance.

Syntax

system-max ip-vrf-route *num*

no system-max ip-vrf-route *num*

Command Default

By default, the maximum number of IPv4 routes per VRF instance are not configured.

Parameters

num

The number of IPv4 routes that can be created per VRF instance. Valid IPv4 route values are 128 through 524288. The default value is 1024.

Modes

Global configuration mode.

Usage Guidelines

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured **system-max** command does not take effect during a hitless-reload.

Use the **no** form of the command to reset the maximum number of IPv4 routes that was configured for a VRF instance.

Examples

The following example configures 200 IPv4 routes per VRF instance.

```
device# configure terminal
device(config)# system-max ip-vrf-route 200
```

History

Release version	Command history
5.8.00	This command was modified.

system-max rstp

Defines the maximum number of Rapid Spanning Tree Protocol (RSTP) instances that can be configured on the Brocade NetIron XMR and MLX Series devices.

Syntax

system-max rstp *number-of-instances*

no system-max rstp *number-of-instances*

Parameters

number-of-instances

Specifies the maximum number of RSTP instances that can be configured on a Brocade device. The valid number of instances are 1 through 256. The default value is 32.

Modes

Global configuration mode

Usage Guidelines

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured **system-max** command does not take effect during a hitless-reload.

The **no** form of the command removes the configured RSTP instances.

NOTE

Before you downgrade from Brocade NetIron Release 5.9 to a lower release and restart the device, it is recommended that you reduce the number of RSTP instances to 128 or a lower value using the **system-max rstp** command. However, if you upgrade from Brocade NetIron Release 5.8 (or previous releases) to 5.9 and restart, there is no change in the RSTP configuration or operation since the lower number of RSTP instances are anyway supported.

Examples

The following example enables configuring a maximum of 48 RSTP instances on the device.

```
device# configure terminal
device(config)# system-max rstp 48
```

History

Release version	Command history
5.9.00	This command was modified to increase the maximum valid RSTP instances from 128 to 256.

system-max trunk-num

Specifies the maximum number of trunks that can be set in the Brocade devices.

Syntax

system-max trunk-num *value*

no system-max trunk-num *value*

Command Default

If this command is not entered, the default number is 128.

Parameters

value

Specifies the maximum number of trunks that can be set on a Brocade device. The valid values are 32, 64, 128, and 1024. The default value is 128.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the previously specified maximum number of trunks.

NOTE
Using this command requires a system restart in order for the new setting to take effect.

Examples

The following example sets the maximum number of trunks to 64.

```
device# configure terminal
device(config)# system-max trunk-num 64
```

History

Release version	Command history
5.4.00a	This command was introduced.

system-max tvf-lag-lb-fid-group

Configures maximum FID group size for transparent VLAN flooding LAG load balancing globally.

Syntax

system-max tvf-lag-lb-fid-group *number*

no system-max tvf-lag-lb-fid-group

Command Default

The default maximum FID group size is 2.

Parameters

number

Specifies the decimal value of the FID number defined per group. Valid values are 2, 4, 8.

Modes

Global configuration mode

Usage Guidelines

The system-max tvf-lag-lb-fid-group command configures maximum FID group size for transparent VLAN flooding LAG load balancing globally. Valid values defined per group are 2, 4, 8.

NOTE

After configuring group size, execute the **write memory** command and restart the router. Configuring a new maximum FID group size could cause instability on failover.

Use the **no** form of this command to disable the configured max group size.

Examples

The following example configures a max group size of 4 for transparent VLAN flooding LAG load balancing:

```
device(config)# system-max tvf-lag-lb-fid-group 4
```

To disable the max group size configuration, use the following command:

```
device(config)# no system-max tvf-lag-lb-fid-group
```

History

Release version	Command history
5.6.00	This command was introduced.

system-max tvf-lag-lb-fid-pool

Configures maximum FID pool size for transparent VLAN flooding LAG load balancing globally.

Syntax

system-max tvf-lag-lb-fid-pool *number*

no system-max tvf-lag-lb-fid-pool

Parameters

number

Specifies the decimal value of FID pool size defined. The valid values are 0, 512, 1024, 2048, and 4096. The default value is 0. Setting the value as 0 will disable transparent VLAN flooding LAG load balancing globally.

Modes

Global configuration mode

Usage Guidelines

Use the **no system-max tvf-lag-lb-fid-pool** command to disable the pool size configuration.

The **system-max tvf-lag-lb-fid-pool** command configures maximum pool size for transparent VLAN flooding LAG load balancing globally.

NOTE

After configuring pool size execute write memory command and restart the router, else it could cause instability on fail over.

Examples

The following example shows how to configure a pool size of 200 for transparent VLAN flooding LAG load balancing:

```
device(config)# system-max tvf-lag-lb-fid-pool 200
```

The following example shows how to configure a max pool size of 4096 for transparent VLAN flooding LAG load balancing:

```
device(config)# system-max tvf-lag-lb-fid-pool 4096
Reload required. Please write memory and then reload or power cycle the system.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.
```

To disable the max pool size configuration use the following command:

```
device(config)#no system-max tvf-lag-lb-fid-pool
```

History

Release version	Command history
5.6.00	This command was introduced.
5.9.00	This command was modified to add a new FID pool value of 4096.

te-metric

Configures the TE-metric value for an MPLS interface.

Syntax

te-metric*value*

no te-metric*value*

Command Default

No TE-metric value is configured.

Parameters

value

Specifies a number for the value of the TE-metric. The value ranges between 1 and 65535.

Modes

MPLS interface configuration mode

Usage Guidelines

no

Examples

The following example sets the TE-metric configured for an MPLS interface to 5.

```
device# configure terminal
device (config)# router-mpls
device(config-mpls)# mpls-interface ethernet 1/1
device(config-mpls-if-e1000-1/1)# te-metric 5
```

The following example tries to remove the TE-metric but gives an incorrect value. An error message is displayed that specifies the currently configured value. This correct value is then entered in the **no** form to remove the TE-metric value for Ethernet interface 1/1.

```
device# configure terminal
device (config)# router-mpls
device(config-mpls-if-e1000-1/1)#no te-metric 3
Error:TE-metric is configured to a value of 5
device(config-mpls-if-e1000-1/1)#no te-metric 5
```

History

Release version	Command history
5.6.00	This command was introduced.

terminal enable timestamp

Enables and disables the timestamp recording for all show commands for the terminal session of the executed command.

Syntax

terminal enable timestamp [iso8601-format]

no terminal enable timestamp [iso8601-format]

Parameters

iso8601-format

Displays the timestamp in ISO 8601 format: YYYY-MM-DDThh:mm:ssTZD (for example, 1997-07-16T19:20:30+01:00). The format uses the following conventions:
YYYY = Year, four digits
MM = for example, 01 = January
DD = Day of the month, two digits (01 through 31)
hh = Hour, two digits (00 through 23) (am/pm is not allowed)
mm = Minutes, two digits (00 through 59)
ss = Seconds, two digits (00 through 59)
TZD = Time zone designator (Z or +hh:mm or -hh:mm)

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to enable the timestamp recording in the default mode to be displayed at the beginning of each show command output. By default, the timestamp is not displayed in the show command outputs. The timestamp recording is applicable only to the current terminal session, and not saved to the startup configuration. The use of this command can assist with troubleshooting or debugging issues.

The default mode is displayed in the system clock format as HH:MM:SS.MSC TZ Wk Mon Day Year (for example 11:41:45.565 GMT+00 Sat Feb 24 2014). The format uses the following conventions:

HH = Hour, two digits (00 through 23) (in 24- hour format)

MM = Minutes, two digits (00 through 59)

SS = Seconds, two digits (00 through 59)

MSC = Milliseconds, three digits (000 through 999)

TZ = Time zone

Wk = Weekday, three characters (Sat, Sun, Mon, and so on)

Mon = Month, three characters

Day = Day, two digits (01 through 31)

Year = Year, four digits

Prior to NetIron 05.9.00, some existing show commands (for example, **show tasks** and **show cpu utilization**) displayed the timestamp as part of the show command output. When the **terminal enable timestamp** command is enabled, an additional timestamp recording will now appear at the beginning of the show command outputs on the session where the**terminal enable timestamp** command is issued.

The **no** form of the command disables the timestamp recording at the beginning of each show command output.

Examples

The following example enables the timestamp recording in default mode. The recording is displayed in the **show ip interface** command output.

```
device# terminal enable timestamp
device# show ip interface
11:41:45.565 GMT+00 Sat Feb 24 2014
Flags : U - Unnumbered, S - Secondary, US - Unnumbered Secondary, V - VE over VPLS, VS - VE over VPLS
Secondary
Interface       IP-Address      OK?  Method Status     Protocol
VRF                                    FLAG
eth 1/2         100.1.1.1       YES  NVRAM  up         up       default-
vrf
eth 2/8         216.1.1.1       YES  NVRAM  admin/down down     default-
vrf
eth 4/2         42.1.1.1        YES  NVRAM  admin/down down     default-
vrf
mgmt 1          10.25.113.41    YES  NVRAM  up         up       default-
vrf
ve 10           110.1.1.1       YES  NVRAM  up         up       default-
vrf
ve 20           120.1.1.1       YES  NVRAM  up         up       default-
vrf
ve 36           36.1.1.1        YES  NVRAM  down       down     default-
vrf
ve 44           44.1.1.1        YES  NVRAM  down       down     default-
vrf
ve 45           45.1.1.1        YES  NVRAM  down       down     default-
vrf
ve 48           48.1.1.1        YES  NVRAM  down       down     default-vrf
```

The following example enables the timestamp recording in the iso8601 format. The recording is displayed in the **show ip interface** command output.

```
device# terminal enable timestamp iso8601-format
device# show ip interface
 2014-01-13T19:20:30+01:00
Flags : U - Unnumbered, S - Secondary, US - Unnumbered Secondary, V - VE over VPLS, VS - VE over VPLS
Secondary
Interface       IP-Address      OK?  Method Status     Protocol
VRF                                    FLAG
eth 2/1         21.1.1.5        YES  NVRAM  up         up       default-
vrf
eth 4/1         10.1.1.1        YES  manual admin/down down
vrf1
mgmt 1          10.37.73.171    YES  NVRAM  up         up       default-
vrf
ve 101          11.1.1.1        YES  NVRAM  up         up       default-
vrf
ve 101          11.1.2.1        YES  NVRAM  up         up       default-
vrf
ve 102          12.1.1.1        YES  NVRAM  up         up       default-
vrf
ve 103          13.1.1.1        YES  NVRAM  up         up       default-
vrf
ve 106          16.1.1.1        YES  manual up         up
vrf1
```

The **show terminal** command is modified to include the terminal timestamp status when the iso8601 format is enabled.

```
device# show terminal
2015-08-03T21:10:59+00:00
Length: 24 lines
Page display mode (session): disabled
Page display mode (global): enabled
Timestamp: enabled (iso8601 format)
```

History

Release version	Command history
5.9.00	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* }

Command Default

See the parameters section for specific defaults.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPF LSAs are collected into a group and refreshed, check-summed, or aged by the OSPF process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

throttle spf

Specifies start, hold and maximum wait intervals for throttling SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 60000 milliseconds. The default is 0.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

max

Maximum wait time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

Enter the **no timers lsa-group-pacing** to restore the pacing interval to its default value.

Enter **no timers throttle spf** to set 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-ospf router)# 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-ospf router)# timers throttle spf 10000 15000 30000
```

timers (OSPFv3)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) timers.

Syntax

timers { **lsa-group-pacing** *interval* | **spf** *start hold* }

Command Default

Enabled.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check-summed, or aged by the OSPFv3 process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

spf

Specifies start and hold intervals for SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 65535 seconds. The default is 5 seconds.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 65535 seconds. The default is 10 milliseconds.

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-ospf6-router)# 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-ospf6-router)# timers spf 10 20
```

traceroute

Traces the network path of packets as they are forwarded to an IPv4 or IPv6 destination address.

Syntax

traceroute { *ipv4-address* | *hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } } [**maxttl** *value*] [**minttl** *value*] [**numeric**] [**source-ip** *address*] [**timeout** *seconds*] [**vrf** *vrf-name*]

Parameters

ipv4-address
Specifies the IPv4 address of the destination device.

hostname
Specifies the name of the destination (host) device.

ipv6 *ipv6-address*
Specifies the IPv6 address of the destination device.

ipv6-hostname
Specifies the name of the destination (host) device.

maxttl *value*
Maximum TTL value in number of hops.

minttl *value*
Minimum TTL value in number of hops.

numeric
Displays the IP address in numeric format.

source-ip *address*
Specifies the IPv4 or IPv6 address of the source device.

timeout *seconds*
The traceroute timeout value.

vrf *vrf-name*
Name of the VRF.

Modes

User EXEC mode

Usage Guidelines

Use the **traceroute** command to help troubleshoot networking issues with packets. If no VRF is specified, the default-vrf is used.

If the source address is an IPv6 link-local address, the destination address must be no more than one hop away in the network. An IPv6 link-local address cannot be routed.

Examples

The following example performs an IPv4 traceroute.

```
device# traceroute 172.16.4.80

traceroute to 172.16.4.80 (172.16.4.80), 64 hops max
 1   10.24.80.1 (10.24.80.1) 0.588ms 0.139ms 0.527ms
 2   10.31.20.61 (10.31.20.61) 0.550ms 0.254ms 0.234ms
 3   10.16.200.113 (10.16.200.113) 0.408ms 0.285ms 0.282ms
 4   10.110.111.202 (10.110.111.202) 5.649ms 0.283ms 0.288ms
 5   10.130.111.38 (10.130.111.38) 1.108ms 0.712ms 0.704ms
 6   10.192.0.42 (10.192.0.42) 37.053ms 32.985ms 41.744ms
 7   172.16.56.10 (172.16.56.10) 33.110ms 33.349ms 33.114ms
 8   172.16.4.9 (172.16.4.9) 34.096ms 33.023ms 33.122ms
 9   172.16.4.80 (172.16.4.80) 76.702ms 83.293ms 79.570ms
```

The following example performs an IPv6 traceroute, with configured minimum and maximum TTL values and a source IP device address.

```
device# traceroute ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 maxttl 128 minttl 30 source-ip 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
5.9.00	This command was modified to add the **source-ip** option for IPv6.

traceroute mpls ldp

Sends an MPLS echo request from the ingress to the egress Label Switching Router (LSR).

Syntax

traceroute mpls ldp { *ip_addr*/*mask_length* } [**destination** *ip_addr*] | [**dsmap**] | [**min-ttl** *min_num*] | [**max-ttl** *max_num*] | [**reply-mode router-alert**] | [**reply-tos** *num*] | [**size** *bytes*] | [**source** *ip_addr*] | [**timeout** *msec*] | [**nexthop** *ipv4_addr*]

Parameters

ip_addr mask_length

Specifies the LDP IPv4 destination prefix and mask length. If the mask-length is not specified, the default value is 32.

destination *ip_addr*

Sets the destination IP address within the 127/8 subset. The default address is 127.0.0.1.

dsmap

Enables the Downstream (DS) mapping TLV in the echo request for traceroute operation.

min-ttl *min_num*

Specifies a minimum value in the min-num variable for the outermost label in the traceroute operation. The default minimum TTL value is one. Acceptable configuration values are 1 - 255.

max-ttl *max_num*

Specifies a maximum value in the max-num variable for the outermost label in traceroute operation. The default maximum TTL value is 30. Acceptable configuration values are 1 - 255.

reply-mode

Used when the normal IP return path is unreliable.

router-alert

This option indicates that the reply must be sent as an IPv4 UDP packet with the Router Alert option. This option requires extra overhead processing at each LSR along the return path.

reply-tos *num*

Specifies to include a TOS value between 0 and 254 in the Reply-TOS-byte TLV. This value copies to the IP header TOS byte of the echo reply. By default, the reply-tos TLV is not included in the Echo Request.

NOTE

The last bit of the TOS byte is always zero.

size *bytes*

Specifies that the size of the echo request, including the label stack to be sent, and will be the value of the variable bytes. The pad TLV is used to fill the echo request message to the specified size. The minimum size is 92 bytes for an MPLS Echo Request. The maximum size is the size of the LSP MTU.

source *ip_addr*

Specifies the IP address of any interface. This address is used as the destination address for the echo reply address. The default address is the LSR ID.

timeout *msec*

Specifies an interval in milliseconds for the echo request message. The default timeout is five seconds. The maximum timeout value is five minutes.

nexthop *ipv4_addr*

Specifies the nexthop IPv4 address that will be used to send the traceroute request. If there is no matching interface for the specified IPv4 address, the traceroute request fails.

Modes

Privileged EXEC mode

Usage Guidelines

You can specify the next hop IPv4 address used to send the traceroute request. If there is no matching interface for the specified IPv4 address, the traceroute request fails. When an address that does not match the outgoing path for the tunnel is given, the following error message appears as a response: Traceroute fails: LDP next-hop does not exist.

Examples

The following example displays the output returned when using the **traceroute mpls ldp** command.

```
device# traceroute mpls ldp 10.22.22.22
Trace LDP LSP to 10.22.22.22/32, timeout 5000 msec, TTL 1 to 30
Type Control-c to abort
1 10ms 10.22.22.22 return code 3(Egress)
```

History

Release Version	Command history
5.5.00	This command was modified to include the **nexthop** keyword.

track-port

Configures network reachability tracking for a specific Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) port.

Syntax

track-port { **ethernet** *slot*/*port* | **pos** *slot*/*port* | **ve** *num* | **tunnel** *tunnel-id* [**priority** *num*]}

no track-port { **ethernet** *slot*/*port* | **pos** *slot*/*port* | **ve** *num* | **tunnel** *tunnel-id* [**priority** *num*]}

Command Default

The network reachability of VRRP and VRRP-E ports or IPsec tunnels is not tracked.

Parameters

ethernet *slot port*

Configures network reachability tracking for a specific Ethernet interface. A forward slash "/" must be entered between the slot and port numbers.

pos *slot port*

Configures network reachability tracking for a specific POS interface. A forward slash "/" must be entered between the slot and port numbers.

tunnel *tunnel-id*

Configures network reachability tracking for an IPsec tunnel. Valid values range from 1 through 254.

ve *number*

Configures network reachability tracking for a virtual Ethernet interface. Valid values range from 1 through 255.

priority *num*

Sets the track priority. Valid numbers are from 1 through 254. The tracking priority number is used when a tracked interface up or down event is detected. For VRRP, if the tracked interface becomes disabled, the current router priority is reduced to the track-port priority. (For VRRP only, interface tracking does not have any effect on an owner router; the owner priority can not be changed under configuration from 255.) For VRRP-E, if the tracked interface becomes disabled, the current router priority is reduced by the track-port priority. For VRRP, the default is 2, and for VRRP-E, the default is 5.

Modes

VRID interface configuration mode

Usage Guidelines

This command can be used to track interfaces and IPsec tunnels for VRRP or VRRP-E. IPsec tunnel tracking is supported for IPv4 VRRP and IPv4 or IPv6 VRRP-E. IPv6 VRRP does not support IPsec tunnels.

For VRRP, the tracked interface can be any valid Ethernet, or virtual Ethernet interface other than the one on which this command is issued. The maximum number of interfaces you can track per virtual router is 8.

Enter the **no track-port** command with the specified options to remove the tracked port configuration.

Examples

The following example configures network reachability tracking on Ethernet interface 2/4.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e10000-1/6)# ip vrrp vrid 1
device(config-if-e10000-1/6-vrid-1)# track-port ethernet 2/4
```

The following example configures network reachability tracking on IPsec tunnels 1 and 2.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e10000-1/6)# ip address 10.53.5.1/24
device(config-if-e10000-1/6)# ip vrrp vrid 1
device(config-if-e10000-1/6-vrid-1)# track-port tunnel 1 priority 40
device(config-if-e10000-1/6-vrid-1)# track-port tunnel 2 priority 30
```

History

Release version	Command history
6.0.0	This command was modified to add an option to track IPsec tunnels.

track-port (VSRP)

Configures the VRID on one interface to track the link state of another interface on the device.

Syntax

track-port ethernet *slot/port* **priority** *number*

track-port ethernet *slot/port* **priority** *number*

Command Default

The VRID does not track an interface.

Parameters

ethernet *slot/port*

Configures the Ethernet interface to track.

priority *number*

Changes the VSRP priority of the interface. The range is from 1 through 255.

Modes

VSRP VRID configuration mode

Usage Guidelines

Configuring this command is useful for tracking the state of the exit interface for the path for which the VRID is providing redundancy.

If the interface configured for tracking goes down, the VSRP VRID priority is reduced by the amount of the track port priority you specify.

The **priority** option changes the priority of the specified interface, overriding the default track port priority. To change the default track port priority, use the **backup track-priority** command.

The **no** form of the command removes the link state tracking.

Examples

The following example configures the VRID to track an Ethernet interface .

```
device(config)# vlan 200
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# track-port ethernet 1/2
```

transparent-hw-flooding lag-load-balancing

Configures transparent VLAN flooding LAG load balancing on a specific VLAN when there is PBR to TVF VLAN flooding.

Syntax

transparent-hw-flooding lag-load-balancing

Command Default

By default, transparent VLAN flooding LAG load balancing is not configured on a specific VLAN with flooding.

Modes

VLAN configuration mode

Usage Guidelines

The **transparent-hw-flooding lag-load-balancing** command configures transparent VLAN flooding LAG load balancing on a specific VLAN when there is PBR to TVF VLAN flooding. The command supports 480 TVF LAG instances.

Use the **no** form of the command to disable the transparent VLAN flooding LAG load balancing on a specific VLAN.

Examples

The following example enables transparent VLAN flooding LAG load balancing on VLAN 100:

```
device(config)# vlan 100
device(config-vlan-100)# transparent-hw-flooding lag-load-balancing
```

To disable transparent VLAN flooding LAG load balancing on VLAN 100, use the following command:

```
device(config)# vlan 100
device(config-vlan-100)# no transparent-hw-flooding lag-load-balancing
```

History

Release Version	Command History
5.6.00	This command was introduced.

transport-address interface

Sets the interface IP address as the LDP transport address. The IP address is used for a TCP connection of the LDP interface.

Syntax

transport-address interface

Command Default

The default is to use the LSR-ID.

Modes

MPLS interface ldp parameter mode (config-mpls-if-*xxx* -ldp-param).

Usage Guidelines

Use the primary address of this interface as LDP transport address

Executing this command causes the LDP session to re-start using the primary interface IP address as the transport address.

Executing the command causes an existing LDP session that is on to go down and come back UP (if this was the only adjacency).

This command can be enabled before or after the **ldp-enable** command on the interface.

Examples

the following example shows when executing the command, it causes an existing LDP session that is on to go down and come back UP (if this was the only adjacency).

```
device>enable
device# configure terminal
device(config)# router mpls
device(config-mpls)# mpls-interface ethernet 1/1
device(config-mpls-if-e1000-1/1)# ldp-params
device(config-mpls-if-e1000-1/1-ldp-params)# transport-address interface
```

History

Release version	Command history
6.1.00	This command was introduced.

tunnel destination

Configures the tunnel destination of the tunnel to the specified IPv6 address. IPv6 packets transmitted across the tunnel are received by this address.

Syntax

tunnel destination *ipv6-address*

no tunnel destination *ipv6-address*

Command Default

This command is not configured.

Parameters

ipv6-address

Specifies the IPv6 address to be the destination of the IPsec IPv6 tunnel.

Modes

Tunnel interface configuration mode

Usage Guidelines

The **no** form of this command removes the specified IPv6 address as the tunnel destination.

Link-local address cannot be used as the destination of the tunnel.

Examples

This example shows configuring the tunnel destination for tunnel number 1 (one) to the IPv6 address of 10:1:1::2/64.

```
device(config) interface tunnel 1
device(config-tnif-1)# tunnel destination 10:1:1::2/64
```

History

Release version	Command history
5.9.00	This command was introduced.

tunnel mode ipsec ipv4

Configures the tunnel mode for the specified tunnel to be IPsec IPv4. This enables support for IPSec on the IPv4 packets transmitted across the tunnel.

Syntax

tunnel mode ipsec ipv4

no tunnel mode ipsec ipv4

Command Default

IPSec is not supported on IPv4 packets transmitted across a tunnel.

Modes

Tunnel interface configuration mode

Usage Guidelines

While this command sets IPSec support for IPv4 packets across a tunnel, use the related **tunnel mode ipsec ipv6** command to set IPsec support for IPv6 packets across a tunnel.

The **no** form of this command disables the IPSec IPv4 support on the specified tunnel.

Examples

The following example configures the tunnel mode for tunnel number 1 (one) to IPSec IPv4.

```
device# configure terminal
device(config) interface tunnel 1
device(config-tnif-1)# tunnel mode ipsec ipv4
```

History

Release version	Command history
05.8.00	This command was introduced.

tunnel mode ipsec ipv6

Configures the tunnel mode for the specified tunnel to be IPsec IPv6. This enables support for IPSec on the IPv6 packets transmitted across the tunnel.

Syntax

tunnel mode ipsec ipv6

[no] tunnel mode ipsec ipv6

Command Default

This command is not configured.

Modes

Tunnel interface configuration mode

Usage Guidelines

The **no** form of this command disables the IPSec IPv6 support on the specified tunnel.

Use the **tunnel mode ipsec ipv4** command to set the tunnel mode to IPsec IPv4.

Examples

The following example configures the tunnel mode for tunnel number 1 (one) to IPSec IPv6.

```
device(config) interface tunnel 1
device(config-tnif-1)# tunnel mode ipsec ipv6
```

History

Release version	Command history
5.9.00	This command was introduced.

tunnel override-pkt-tos-ttl

Configures the IPsec tunnel to copy the configured TOS and TTL values to the outer IP header.

Syntax

tunnel override-pkt-tos-ttl

no tunnel override-pkt-tos-ttl

Command Default

By default, when a packet goes out on an IPsec tunnel, the TOS and TTL values are copied from the inner IP header to the outer IP header.

Modes

Tunnel interface configuration mode

Usage Guidelines

The **no** form of the command disables the IPsec tunnel from copying the TOS and TTL values.

Examples

The following example configures the IPSec tunnel interface to copy the TOS and TTL values.

```
device(config)# interface ethernet 3/1
device(config-int-e10000-3/1)# ip address 36.0.8.108/32
device(config-int-e10000-3/1)# interface tunnel 1
device(config-tnif-1)# tunnel override-pkt-tos-ttl
```

History

Release version	Command history
05.8.00	This command was introduced.

tunnel protection ipsec profile

Configures an IPsec profile for an IPsec virtual tunnel interface (VTI).

Syntax

tunnel protection ipsec profile *ipsec-profile-name*

no tunnel protection ipsec profile *ipsec-profile-name*

Command Default

An IPsec profile is not configured for the VTI.

Parameters

ipsec-profile-name

Specifies the name of the IPsec profile to secure packets that go out on this interface.

Modes

Interface configuration mode

Usage Guidelines

This command can be used for both IPsec IPv4 and IPsec IPv6 tunnels.

Before executing this command, the tunnel mode must be set to ipsec by using the **tunnel mode ipsec** command.

The **no** form of the command removes the IPsec profile configuration.

Examples

The following example shows how to configure an IPsec profile named ipsec1 on interface 3/1 (the tunnel identifier is 1). This example is for an IPsec IPv4 tunnel.

```
device# configure terminal
device(config)# interface ethernet 3/1
device(config-int-e10000-3/1)# ip address 36.0.8.108/32
device(config-int-e10000-3/1)# interface tunnel 1
device(config-tnif-1)# tunnel protection ipsec profile ipsec1
```

History

Release version	Command history
05.8.00	This command was introduced.
05.9.00	This command was modified to support IPsec IPv6 tunnels.

tunnel source

Configures the tunnel source of the tunnel to the specified IPv6 address. IPv6 packets are forwarded from this address across the tunnel.

Syntax

tunnel source *ipv6-address*

no tunnel source *ipv6-address*

Command Default

This command is not configured.

Parameters

ipv6-address

Specifies the IPv6 address to be the source of the IPsec IPv6 tunnel.

Modes

Tunnel interface configuration mode

Usage Guidelines

The **no** form of this command removes the specified IPv6 address as the tunnel source.

Link-local address cannot be used as the source of the tunnel.

Examples

This example shows configuring the tunnel source for tunnel number 1 (one) to the IPv6 address of 10:1:1::1/64.

```
device(config) interface tunnel 1
device(config-tnif-1)# tunnel source 10:1:1::1/64
```

History

Release version	Command history
5.9.00	This command was introduced.

tunnel-interface

Configures the LSP tunnel's interface index.

Syntax

tunnel-interface { *index* }

no tunnel-interface { *index* }

Command Default

There is no specific default for this command. If not configured, an unused value is chosen.

Parameters

index

Decimal value. The range is system dependent. For XMR/MLXe-MR2 systems, the range is 1 - 16384. For CES/CER systems, the range is 1 - 1024.

Modes

MPLS LSP and MPLS bypass LSP modes (config-mpls-lsp*x*).

Usage Guidelines

The **no** option frees the tunnel-interface configured for this node and has a new value dynamically allocated. If the next available index value is the same as that just removed by the user, the same value is still allocated. This is not an error condition. The main purpose of this command is for scenarios where the user wants to allocate any value to the LSP and not something chosen by the user.

The picking algorithm uses the least index that is unused. If none are available (in cases where the number of LSPs supported has been exceeded), the LSP is not allowed to be created. If the user configures a value, there is a check to see if the value is unused or is in use by this tunnel already. If it is in use by another LSP, an error displays and the user will have to configure another value. If it is free, the current value is freed up to be used by any other LSP and the configured value is taken up by this LSP.

This command can be executed irrespective of the state of the LSP - enabled or disabled. It does not depend on adaptive and does not need a commit. The interface index value is for the tunnel and is shared by all the paths - secondary or primary.

Special case handling:

Error handling in the special cases that the user loads a startup-configuration that have the following errors:

1. Multiple LSPs configured with the same tunnel-interface index.

1. In this scenario, the LSPs that comes up later will come up as before.
2. These LSPs do not have a valid tunnel-interface value and cannot be queried using SNMP.
3. In the **show mpls lsp** detail view, the tunnel-interface index is shown as "Invalid". LSP c2, to 3.3.3.3, tunnel-interface index: Invalid.

4. Only the first LSP to get the value has the valid tunnel-interface index.
5. The configuration continues to show the configured incorrect value, and the user can change it to a valid unused value.
6. The user can list all LSPs that have an invalid tunnel-interface index using the command - **show mpls lsp invalid-tunnel-interface**.

    2. Multiple LSPs without a tunnel-interface configured.

a. LSPs that do not have a value configured in the Configuration are allocated to a tunnel-interface index.
b. It is possible that a later LSP might have configured on it the same value allocated to an LSP as in step 2a.
c. In such a scenario, de-allocate the index of the first LSP and allocate that value to the later LSP. The former is then allocated a new value from the free indexes.

NOTE
The above cases apply *only* to errors in the startup-configuration, not in the case of execution of the CLI during normal running.

Examples

The following example shows how to configure the LSP tunnel interface index:

```
device#configure terminal
device(config)#router mpls
device(config-mpls)#lsp lsp1
device(config-mpls-lsp1)#tunnel-interface 100
device(config-mpls-lsp1)#to 3.3.3.3
device(config-mpls-lsp1)#enable

device#configure terminal
device(config)#router mpls
device(config-mpls)#bypass-lsp byp1
device(config-mpls-bypasslsp-byp1)#tunnel-interface 102
device(config-mpls-bypasslsp-byp1)#to 3.3.3.3
device(config-mpls-bypasslsp-byp1)#exclude-interface eth 2/1
device(config-mpls-bypasslsp-byp1)#enable
```

History

Release version	Command history
5.9.00	This command is introduced.

tvf-domain

Creates a transparent VLAN flooding (TVF) domain that provides an infrastructure to support up to 2016 TVF instances with LAG load balancing.

Syntax

tvf-domain *tvf-domain-ID* [**name** *tvf-domain-name*]

no tvf-domain *tvf-domain-ID* [**name** *tvf-domain-name*]

Parameters

tvf-domain-ID
Specifies the ID of the TVF domain. Valid values are from 1 through 2016.

name *tvf-domain-name*
Specifies the name of the TVF domain. The name can be up to 64 characters in length.

Modes

Global configuration mode

Usage Guidelines

The TVF domain supports only TVF with LAG load balancing.

The **no** form of the **tvf-domain** *tvf-domain-ID* [**name** *tvf-domain-name*] command removes only the name and the TVF domain ID remains the same without a name.

The **no** form of the **tvf-domain** command removes the TVF domain.

Examples

The following example configures a named TVF domain.

```
device# configure terminal
device(config)# tvf-domain 1 name domainuser
```

History

Release version	Command history
6.0.00	This command was introduced.

tx-label-silence-timer

Sets the length of the EOL transmit label silence timer for LDP-IGP synchronization.

Syntax

tx-label-silence-timer *milliseconds*

no tx-label-silence-timer

Command Default

The default value is 1000 milliseconds.

Parameters

milliseconds

Specifies the EOL transmit label silence timer in milliseconds. Enter an integer from 100 to 60000.

Modes

MPLS LDP EOL configuration mode

Usage Guidelines

Use the **no** form of the resets the default value of 1000 milliseconds.

Examples

The following example sets the length of time for the EOL transmit label silence timer to 2000 milliseconds.

```
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# end-of-lib
device(config-mpls-ldp-eol)# tx-label-silence-timer 2000
```

uda access-group

Binds the user defined ACL table to any physical port.

Syntax

uda access-group { [*access-list_name* | *uda-acl num*] [**in**] | **enable-deny-logging** [**hw-drop**] }

no uda access-group { [*access-list_name* | *uda-acl num*] [**in**] | **enable-deny-logging** [**hw-drop**] }

Parameters

access-list_name
: Specifies the selected access list by name.

uda-acl num
: Specifies the selected UDA access list by the UDA ACL number. The numbere must be between 2000 - 2999.

in
: Specifies inbound packets.

enable-deny-logging
: Enables UDA ACL logging on the port.

hw-drop
: Drops the ACL deny log packet in the hardware.

Modes

User sub-configuration mode (configuration-interface-ethernet).

Usage Guidelines

The user defined ACL created must be passed to this CLI command.

Only the user defined ACLs are supported in the ingress side. The UDA offsets must be defined for the access list before binding the ACL to any physical port. If not, the error message **"UDA offsets are not defined for this port"** displays and binding fails.

All the UDA ACL clauses defined in the UDA ACL table are programmed into the hardware. The UDA offsets configured as "ignore" are masked in the ACL rule while programming in the hardware.

If the empty UDA ACL is bound to a physical port, the UDA ACL lookup will not happen until additional rules are added.

The **no** form of the command removes the binding of the user defined ACL table to any physical port.

Examples

The following example displays the output by number.

```
device (config)# show access-list uda
UDA Access List 2000:
10: access-list 2000 permit 100 any any 00001122 0000ffff 00003344 0000ffff
20: access-list 2000 permit any any any any any
!
UDA Access List 2001:
10: access-list 2001 permit 200 any any 00001122 0000ffff 00003344 0000ffff
20: access-list 2001 permit any any any any any
!
```

The following example displays the output by name.

```
device(config)# show access-list uda TestUdaAcl
UDA Access List TestUdaAcl:
access-list 2000 uda-offsets 12     20     36       72
10: access-list 2000 permit 100 any any 00001122 0000ffff 00003344 0000ffff
20: access-list 2000 permit any any any any any
!
```

History

Release version	Command history
5.9.00	This command was introduced.

uda-offsets

Defines the User Defined fields offset values. This is configured in the physical interface.

Syntax

uda-offsets [**offset0** | **ignore**] [**offset1 ignore**] [**offset2 ignore**] [**offset3 ignore**]

no uda-offsets [**offset0** | **ignore**] [**offset1 ignore**] [**offset2 ignore**] [**offset3 ignore**]

Command Default

Parameters

offset1

The offset specified is the offset from the beginning of the normalized packet. The maximum value of the offset is 116.

ignore

Ignore offset1.

Modes

User configuration mode (interface-ethernet).

Usage Guidelines

If the offsets are not in the 4 byte boundary or greater than 116, an error message "UDA Offset0 'value' is invalid. The Specify Value is in 32-bit boundary and < 116" displays.

The UDA offsets can be modified when the UDA ACL is bound to the physical port. The UDA ACL rules dynamically update to mask the "ignored" UDA fields.

Deleting uda-offsets when some UDA ACL bound to the physical port is not allowed and an error is displayed (**UDA ACL <id> is bound to this port <slot/port>. Unbind UDA ACL before modifying uda-offsets**).

The **no** form of the command removes the uda-offset configuration on the specified UDA Table.

Examples

The following example displays how to define up to four offsets.

```
device configure terminal
device(config)# interface ethernet 1/1
device(config-intf-e1000-1/1)# uda-offsets  0  4  8 12
```

The following example displays how to define two offsets.

```
device configure terminal
device(config)# interface ethernet 1/1
device(config-intf-e1000-1/1)# uda-offsets  0  4 ignore ignore
```

The following example displays how to remove the uda-offset configuration on the specified UDA table.

```
device configure terminal
device(config)# interface ethernet 1/1
device(config-intf-e1000-1/1)# no uda-offsets
```

History

Release version	Command history
5.9.00	This command was modified to define a User Defined fields offset values.

underflow-limit

Sets the number of consecutive samples which have to be below the threshold value to trigger a premature adjustment to the reserved bandwidth of the label-switched path (LSP).

Syntax

underflow-limit *value*

no underflow-limit *value*

Command Default

The default is that there is no premature adjustment because of underflow.

Parameters

value

Defines the number of consecutive samples. Default is 0.

Modes

MPLS autobw-template config mode

MPLS LSP mode

Usage Guidelines

In the auto-bandwidth feature, the traffic rate through an LSP is sampled and the reserved bandwidth of the LSP is automatically changed through a make-before-break mechanism. This is done in order to keep the reserved bandwidth close to the actual traffic rate. It is beneficial to have an optimum bandwidth reservation for an LSP. Auto-bandwidth allows for a very efficient use of network-bandwidth. Use the **underflow-limit** command to reduce the reserved bandwidth prematurely, when the actual traffic rate is consistently much lower than the current reserved bandwidth.

This command can be entered in several modes, under MPLS auto-bandwidth template configuration mode or in MPLS LSP mode as shown in the examples section.

The **no** function of the command sets the underflow-limit back to the default value.

Examples

The following example sets the underflow-limit in an auto-bandwidth template.

```
device(config)# router mpls
device(config-mpls)# autobw-template template1
device(config-mpls-autobw-template-template1)# underflow-limit 10
```

The following example sets the underflow-limit for an individual LSP.

```
device(config)# router mpls
device(config-mpls)#lsp lsp1
device(config-mpls-lsp-lsp1)# autobw-threshold-table
device(config-mpls-lsp-lsp1-autobw)# underflow-limit 10
```

The following example clears the underflow-limit configuration. The user issues the same command with the **no** option. The underflow-limit configuration is set back to the default value of zero (0).

```
device(config-mpls-autobw-template-template1)# no underflow-limit 10
device(config-mpls-lsp-lsp1-autobw)# no underflow-limit 10
```

History

Release	Command history
5.6.00	The command was introduced.

update-lag-name

Modifies an existing Link Aggregation Group (LAG) name without deleting and recreating the configured LAG.

Syntax

update-lag-name *new-name*

Parameters

new-name

Specifies the new LAG name for an existing LAG name. The LAG name can contain up to 64 characters.

Modes

LAG configuration mode

Usage Guidelines

The modified LAG name should be unique across all the LAG names that are available. This command works for all LAG types, such as static, dynamic, and keepalive LAGs.

Examples

The following example changes the existing LAG name from "blue" to "brocade."

```
device# configure terminal
device(config)# show run
device(config)# lag blue
device(config-lag-blue)# update-lag-name brocade
```

The following partial output verifies the update of the existing LAG name from "blue" to "brocade."

```
device(config)# show run
!Current configuration:
module 3 br-mlx-24-port-1gc-x
!
!
lag "blue" static id 2
 ports ethernet 3/1
 primary-port 3/1
 deploy
!
!
device(config)# lag blue
device(config-lag-blue)# update-lag-name brocade
device(config-lag-brocade)# show run
!Current configuration:
!
module 3 br-mlx-24-port-1gc-x
!
!
!
lag "brocade" static id 2
 ports ethernet 3/1
 primary-port 3/1
 deploy
```

History

Release version	Command history
5.9.00	This command was introduced.

use-v2-checksum

Enables the v2 checksum computation method for an IPv4 Virtual Router Redundancy Protocol version 3 (VRRPv3) session.

Syntax

use-v2-checksum

no use-v2-checksum

Command Default

VRRPv3 uses the v3 checksum computation method.

Modes

VRRP configuration mode

Usage Guidelines

The **no** form of this command enables the default v3 checksum computation method in VRRPv3 sessions.

Some non-Brocade devices only use the v2 checksum computation method in VRRPv3. This command enables the v2 checksum computation method in VRRPv3 and provides interoperability with these non-Brocade devices.

Examples

The following example shows the v2 checksum computation method enabled for an VRRPv3 IPv4 session on a Brocade device.

```
device# config
device(config)# router vrrp
device(config)# ethernet 2/4
device(config-if-e1000-2/4)# ip vrrp vrid 14
device(config-if-e1000-2/4-vrid-14)# version v3
device(config-if-e1000-2/4-vrid-14)# use-v2-checksum
device(config-if-e1000-2/4-vrid-14)# ip-address 10.14.14.99
device(config-if-e1000-2/4-vrid-14)# activate
```

History

Release version	Command history
5.7.00	This command was introduced for IPv6 VRRPv3 sessions running on NetIron device images.
5.8.00	This command was modified to support IPv4 and IPv6 VRRPv3 sessions running on NetIron device images.

use-vrrp-path

Suppresses RIP advertisements for interfaces on which Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) backup routers are configured.

Syntax

use-vrrp-path

no use-vrrp-path

Command Default

RIP advertisements are sent from the backup router interface.

Modes

RIP router configuration mode

Usage Guidelines

A VRRP backup router includes route information for the interface that is backing up in RIP advertisements. As a result, other routers receive multiple paths for the interface and might unsuccessfully use the path to the backup router rather than the path to the master router. If the VRRP backup routers are suppressed from advertising the backed-up interface in RIP, other routers learn only the path to the master router for the backed-up interface.

The **no** form of this command resets the default behavior and RIP advertisements are sent from the backup router interface.

Examples

The following example enables RIP advertisement suppression for information about interfaces on VRRP or VRRP-E backup routers.

```
device# configure terminal
device(config)# router rip
device(config-rip-router)# use-vrrp-path
```

The following example disables RIP advertisement suppression.

```
device# configure terminal
device(config)# router rip
device(config-rip-router)# no use-vrrp-path
```

version

Sets the version number for a Virtual Router Redundancy Protocol (VRRP) session.

Syntax

version { **v2** | **v3** }

no version { **v2** | **v3** }

Command Default

VRRP version 2 is the default.

Parameters

v2

Configures VRRP version 2 for this session.

v3

Configures VRRP version 3 for this session.

Modes

Virtual routing ID interface configuration mode

Usage Guidelines

The **no** form of this command resets the VRRP session to the default of version 2.

VRRP version 2 supports IPv4 addresses, and VRRP version 3 supports both IPv4 and IPv6 addresses.

NOTE
Mixed mode (VRRPv2 and VRRPv3) is not supported in the same VRRP virtual routing ID (VRID) session.

Examples

The following example sets VRRP routing instance VRID 1 to version 3.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# version v3
```

virtual-mac

Enables the manual generation of a virtual MAC address for a Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) instance.

Syntax

virtual-mac { *mac-address* | *ipv6-mac-address* }

no virtual-mac { *mac-address* | *ipv6-mac-address* }

Command Default

If there is no manually configured virtual MAC address for a VRRP or VRRP-E instance, the system automatically assigns a virtual MAC address.

Parameters

mac-address

Configures a unique virtual MAC address for an IPv4 VRRP or VRRP-E instance using hexadecimal.

ipv6-mac-address

Configures a unique virtual MAC address for an IPv6 VRRP or VRRP-E instance using hexadecimal.

Modes

VRRP-Extended group configuration mode

Usage Guidelines

By default, the VRRP or VRRP-E virtual MAC is derived as **02:e0:52:***<2-byte-ip-hash>***:***<1-byte-vrid>*

NOTE

System-assigned virtual MAC addresses and manually configured virtual MAC addresses can exist at the same time on the device under the same VRID, but the configured value takes precedence. When the configured value is deleted, the assigned value again applies.

Examples

The following example enables the generation of a virtual MAC with 0 IP hash:

```
device# configure terminal
device(config)# interface ve 10
device(config-ve-10)# vrrp-extended-group 100
device(config-vrrp-extended-group-100)# virtual-mac aaa.bbbb.cccc
```

vll

Defines virtual leased line service and supports inter-operation between vendors.

Syntax

vll *name vll_id* [**cos** *num* | **raw-mode** [**cos** *num*] | **raw-pass-through-mode** [**cos** *num*]]

no vll *name vll_id* [**cos** *num* | **raw-mode** [**cos** *num*] | **raw-pass-through-mode** [**cos** *num*]]

Command Default

A virtual leased line service is not configured.

Parameters

name

The name of the VLL. The name may be up to 64 characters.

vll_id

The VLL identifier. The range is from 1 - 4294967294.

cos *num*

Optional COS selection.

raw-mode

Raw-mode Ethernet type (VC type 5) (Default is the Tagged mode with VC type 4).

raw-pass-through-mode

Raw-pass-through-mode Ethernet type (VC type 5 if untagged endpoint and VC type 4 if tagged endpoint).

Modes

MPLS configuration mode

Usage Guidelines

The raw-mode and tagged-mode supports are for both CES and XMR platforms. In the raw-pass-through mode, VLL instance behaves similarly to either tagged-mode or raw-mode based on the VLL endpoint configuration and similar to tagged-mode for a tagged endpoint and raw-mode for an untagged endpoint.

Examples

The following example configures the **raw-pass-though-mode** option.

```
device(config)#
device(config)# router mpls
device(config-mpls)# soft-preemption cleanup-timer
device(config-mpls)# vll test 1
device(config-mpls)# vll test 1 raw-pass-through-mode
device(config-mpls-vll-test)# vll-peer 10.0.0.1
device(config-mpls-vll-test)# vlan 100
device(config-mpls-vll-test-vlan-100)# tagged ethernet 1/12
device(config-mpls-vll-test-vlan-100)#
```

History

Release version	Command history
5.5.00	This command was modified to include the **raw-pass-though-mode** keyword.

vll-peer

Defines the far-end router IP address of the virtual leased line (VLL).

Syntax

vll-peer *ip_address* [*ip_address* | **ldp** *ip_address* | **lsp** *lsp_name...*]

no vll-peer *ip_address* [*ip_address* | **ldp** *ip_address* | **lsp** *lsp_name...*]

Parameters

ip_address
Specifies the IP address of the VLL peer.

ldp *ip-address*
The destination IP address of an LDP tunnel for the VLL peer.

lsp *lsp_name...*
Specifies LSP assignment for the VLL peer.

Modes

MPLS VLL configuration mode

Usage Guidelines

NOTE
The **ldp** and **lsp** options are mutually exclusive; you can configure either the **ldp** option or the **lsp** option for a VLL peer.

Use the **ldp** option to assign a specific LDP tunnel to a VLL.

Use the **lsp** option to provide a similar user experience as compared to VPLS LSP mapping while at the same time preserving the constructs of VLL peer configurations corresponding to Pseudowire Emulation (PWE) redundancy and MCT-VLL. This approach is backwards compatible. Incremental additions and deletions are allowed.

Up to eight LSP names to a peer can be configured using this command. All eight LSPs are optional. When a VLL peer is not assigned to any LSPs, the default mechanisms for selecting an LSP for the VLL peer are used.

To verify the configuration of this command, use the **show mpls config vll** command with the name of the VLL for which you want to display the configuration.

The **no** form of the command removes the far-end router IP address configuration for a virtual leased line (VLL).

Examples

The following example shows how to assign a specific LDP tunnel to a VLL.

```
device# configure terminal
device(conf)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 10.1.1.1 ldp 10.5.5.5
device# show mpls config vll test
vll test 1000
  vll-peer 10.1.1.1 ldp 10.5.5.5
  vlan 1000
   tagged e 4/5
```

The following example configures a single VLL peer with a set of LSPs.

> **NOTE**
> Configuring the VLL peer and assigning LSPs can be done in the same line.

```
device# configure terminal
device(conf)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
device# show mpls config vll test
vll test 1000
  vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
  vlan 1000
   tagged e 4/5
```

The following example appends an LSP to an existing list of LSPs mapped to a VLL peer.

```
device# configure terminal
device(conf)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp5
```

The following example removes an LSP from an existing list of LSPs for a VLL peer.

```
device# configure terminal
device(conf)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
device(config-mpls-vll-test)# no vll-peer 1.1.1.1 lsp lsp4
device(config-mpls-vll-test)# end
device# show mpls config vll test
vll test 45000
  vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3
  vlan 1000
   tagged e 4/5
```

The following example configures primary and standby VLL peers with a set of LSPs.

> **NOTE**
> When configuring LSPs for primary or standby peers, it is mandatory to configure the peers in advance and then proceed to configure the respective LSPs.

```
device# configure terminal
device(conf)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 2.2.2.2
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
device(config-mpls-vll-test)# vll-peer 2.2.2.2 lsp lspa1 lspa2 lspa3 lspa4
```

The following example removes an LSP from the list of LSPs mapped to a standby VLL peer.

```
device# configure terminal
device(conf)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 2.2.2.2
device(config-mpls-vll-test)# vll-peer 2.2.2.2 lsp lspa1 lspa2 lspa3 lspa4
device(config-mpls-vll-test)# no vll-peer 2.2.2.2 lsp lspa4
```

History

Release version	Command history
5.7.0	This command was modified to add the **lsp** keyword to assign mapped LSPs to the VLL. Up to eight LSPs are now available.
6.0.0	This command was modified to add the **ldp** keyword. The **ldp** keyword assigns a specific LDP tunnel to a VLL.

vrf forwarding

Enables VRF forwarding by configuring a port as a VRF port.

Syntax

vrf forwarding *forwarding-vrf-name*

Parameters

forwarding-vrf-name
Specifies the VRF name.

Modes

Interface tunnel configuration mode

Usage Guidelines

Only GRE IP and IPsec tunnel interfaces are supported as ports that can forward VRF traffic.

Examples

The following example configures VRF forwarding on a device.

```
device(config)# interface ethernet 3/1
device(config-int-e10000-3/1)# ip address 36.0.8.108/32
device(config-int-e10000-3/1)# interface tunnel 1
device(config-tnif-1)# vrf forwarding red
```

History

Release version	Command history
05.8.00	This command was introduced.

vsrp

Configures VSRP on a device.

Syntax

vsrp vrid *vrid-num*

no vsrp vrid *vrid-num*

Command Default

VSRP is not configured.

Parameters

vrid *vrid-num*

Configures the VRID for the VLAN. The VRID range is from 1 through 255.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command clears the VSRP configuration.

Examples

The following example shows how to configure the VRID.

```
device(config)# vlan 200
device(config-vlan-200)# vsrp vrid 1
```

vsrp auth-type

Configures a simple text-string as a password in packets sent on the interface.

Syntax

vsrp auth-type { **no-auth** | **simple-text-auth** *password* }

no vsrp auth-type { **no-auth** | **simple-text-auth** *password*}

Command Default

By default, no authentication is configured.

Parameters

auth-type

Configures the VSRP authentication type.

no-auth

Configures the VRID and interface without authentication.

simple-text-auth *password*

Configures the VRID to use simple text authentication with a password up to 8 characters long.

Modes

VLAN configuration mode

Usage Guidelines

If the interfaces on which you configure the VRID use authentication, the VSRP packets on those interfaces also must use the same authentication.

- No authentication - The interfaces do not use authentication.
- Simple - The interfaces use a simple text-string as a password in packets sent on the interface. If the interfaces use simple password authentication, the VRID configured on the interfaces must use the same authentication type and the same password.

Examples

The following example shows how to configure a simple password.

```
device(config)# vlan 200
device(config-vlan-200)# vsrp auth-type simple-text-auth ourpword
```

vsrp restart-port

Configures a single port on a VSRP-configured device to shut down its port for the specified number of seconds before it starts back up.

Syntax

vsrp restart-port [*seconds*]

no vsrp restart-port *seconds*

Command Default

The default value is 1 second.

Parameters

seconds

Specifies the time the VSRP master shuts down its port before it restarts. The range is from 1 through 120 seconds.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command resets the time to the default value of 1 second.

Examples

The following example configures the ports to restart in 5 seconds.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# vsrp restart-port 5
```

write memory

Saves the current running configuration information to the startup configuration file.

Syntax

write memory

Command Default

Configuration information is not saved to the startup-config file until a **write memory** is performed.

Modes

Privileged EXEC mode

Usage Guidelines

This command saves a configuration change permanently so that the change remains in effect following a system reset or software reload. This command can be entered in any configuration mode, as well as in Privileged EXEC mode.

Some configuration changes like memory allocation changes, require you to reload the software after you save the changes to the startup configuration file.

You should always execute the **write memory** command after making extensive configuration changes. For example, on devices that support stacking any stacking-related configuration changes such as changing priority or stacking ports should be saved to the startup-config file.

NOTE
Keep a backup copy of the startup configuration file in the event of system reset.

Examples

The following example configures a new priority of 255 for stack unit 1, enables the priority, and saves the configuration change to the startup configuration file.

```
device# config terminal
device(config)# stack unit 1
device(config-unit-1)# priority 255
device(config-unit-1)# stack enable
Enable stacking. This unit actively participates in stacking
device(config-unit-1)# write memory
Write startup-config done.
Flash Memory Write (8192 bytes per dot) .Flash to Flash Done.
device(config-unit-1)# end
```