COMMAND REFERENCE GUIDE

RUCKUS FastIron Command Reference, 08.0.30

Supporting FastIron Software Release 08.0.30

Part Number: 53-1003637-22
Publication Date: 17 October 2022

Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **29**
Contacting RUCKUS Customer Services and Support 29
What Support Do I Need? 29
Open a Case 29
Self-Service Resources 30
Document Feedback 30
RUCKUS Product Documentation Resources 30
Online Training Resources 30
Document Conventions 31
Notes, Cautions, and Safety Warnings 31
Command Syntax Conventions 31

About This Document **33**
New in This Document 33
Modified commands for FastIron 08.0.30p 33
Supported hardware and software 33

Using the FastIron command-line interface **35**
Accessing the CLI 35
Command modes 35
Command help 36
Command completion 36
Scroll control 37
Line editing commands 37
Searching and filtering command output 38
Searching and filtering output at the --More-- prompt 38
Searching and filtering show command output 39
Creating an alias for a CLI command 42
Configuration notes for creating a command alias 43
Specifying stack-unit, slot number, and port number 43
Specifying a port on a modular device 43
Specifying a port on stackable devices 43

Commands A - E **45**
100-fx 45
100-tx 46
aaa accounting commands 47
aaa accounting dot1x 49
aaa accounting exec 51
aaa accounting system 53
aaa authentication dot1x 55
aaa authentication enable 56
aaa authentication login 58
aaa authentication snmp-server 60
aaa authentication web-server 62
aaa authorization coa enable 64
aaa authorization coa ignore 65
aaa authorization commands 67

aaa authorization exec ... 69
accept-mode ... 71
access-control vlan ... 73
access-list enable accounting ... 74
access-list deny ... 75
access-list permit ... 77
access-list remark ... 79
accounting ... 80
acl-logging ... 81
acl-mirror-port ... 82
activate (VSRP) ... 84
add mac ... 85
address-family ... 87
address-family unicast (BGP) ... 88
add-vlan ... 90
advertise backup (VSRP) ... 91
age ... 92
aggregate-address (BGP) ... 94
aggregated-vlan ... 96
alias ... 97
all-client ... 99
always-compare-med ... 100
always-propagate ... 101
anycast-rp ... 103
arp-internal-priority ... 105
as-path-ignore ... 106
atalk-proto ... 107
attempt-max-num ... 108
auth-default-vlan ... 109
authenticate ... 111
authenticated-mac-age-time ... 112
authentication ... 113
authentication auth-default-vlan ... 114
authentication auth-order ... 116
authentication auth-vlan-mode ... 118
authentication disable-aging ... 120
authentication dos-protection ... 121
authentication fail-action ... 123
authentication filter-strict-security ... 125
authentication-key ... 127
authentication max-sessions ... 128
authentication reauth-timeout ... 130
authentication source-guard-protection enable ... 131
authentication timeout-action ... 133
auth-fail-action (802.1X authentication) ... 135
auth-fail-action (Flexible authentication) ... 136
auth-fail-force-restrict ... 138
auth-fail-max-attempts ... 139
auth-fail-vlanid ... 141
auth-mode captive-portal ... 142

auth-mode none 143
auth-mode passcode 144
auth-mode username-password 147
auth-order 149
auth-vlan-mode 151
auto-cost reference-bandwidth (OSPF) 153
auto-cost reference-bandwidth (OSPFv3) 155
autosave 157
backup (VSRP) 158
backup-hello-interval (VSRP) 160
bandwidth (interface) 161
banner 163
bgp-redistribute-internal 165
block 166
block-applicant 167
block-learning 169
bootfile 171
bootp-relay-max-hops 172
boot system flash 173
boot system tftp 175
bpdu-flood-enable 176
breakout ethernet 177
bridged-routed 180
broadcast client 181
broadcast destination 182
broadcast limit 183
bsr-candidate 185
buffer-profile port-region 187
buffer-sharing-full 189
capability as4 190
captive-portal 191
captive-portal profile 192
cdp enable 193
cdp run 194
chassis name 195
clear access-list 196
clear access-list accounting 197
clear acl-on-arp 199
clear auth-mac-table 200
clear cable diagnostics tdr 202
clear dhcp 203
clear dot1x mac-sessions 204
clear dot1x sessions 205
clear dot1x statistics 206
clear dot1x statistics 207
clear dot1x-mka statistics 208
clear fdp counters 209
clear fdp table 210
clear gvrp statistics 211
clear ip dhcp-server binding 212

clear ip mroute 213
clear ip pim counters 215
clear ip pim hw-resource 216
clear ip pim rp-map 217
clear ip pimsm-snoop 218
clear ipv6 dhcp-relay delegated-prefixes 219
clear ipv6 dhcp-relay statistics 220
clear ipv6 dhcp6 snooping 221
clear ipv6 mroute 222
clear ipv6 neighbor 223
clear ipv6 pim cache 225
clear ipv6 pim counters 226
clear ipv6 pim hw-resource 227
clear ipv6 pim rp-map 228
clear ipv6 pim traffic 229
clear ipv6 pimsm-snoop 230
clear ipv6 raguard 231
clear ipv6 tunnel 232
clear link-keepalive statistics 233
clear link-oam statistics 234
clear lldp neighbors 235
clear lldp statistics 236
clear logging 237
clear loop-detection 238
clear mac-address 239
clear mac-address cluster 240
clear mac-authentication sessions 241
clear macsec ethernet 242
clear management-vrf-stats 243
clear notification-mac statistics 244
clear openflow 245
clear port security 246
clear public-key 247
clear pvstplus-protect-statistics 248
clear stack ipc 249
clear statistics 251
clear statistics openflow 253
clear webauth vlan 254
clear web-connection 255
clear stp-protect-statistics 256
client 257
client-auto-detect config 258
client-auto-detect ethernet 259
client-auto-detect start 260
client-auto-detect stop 261
client-interface 262
client-interfaces shutdown 263
client-isolation 264
client-to-client-reflection 265
clock 266

cluster ... 267
cluster-id ... 268
compare-routerid ... 269
confederation identifier ... 270
confederation peers ... 271
connect ... 272
console timeout ... 274
copy disk0 ... 276
copy flash console ... 277
copy flash disk0 ... 279
copy flash scp ... 281
copy flash tftp ... 283
copy running-config disk0 ... 284
copy running-config scp ... 285
copy running-config tftp ... 287
copy scp flash ... 288
copy scp license ... 291
copy scp running-config ... 293
copy scp startup-config ... 295
copy startup-config disk0 ... 297
copy startup-config scp ... 298
copy startup-config tftp ... 300
copy tftp flash ... 301
copy tftp running-config ... 303
copy tftp startup-config ... 304
cpu-limit ... 305
critical-vlan ... 306
crypto key client generate ... 307
crypto key client zeroize ... 308
crypto key generate ... 309
crypto key zeroize ... 310
crypto-ssl certificate ... 311
cycle-time ... 312
dampening ... 313
dead-interval (VSRP) ... 315
decnet-proto ... 316
default-gateway ... 317
default-information-originate (BGP) ... 318
default-local-preference ... 319
default-metric (BGP) ... 320
default-ports ... 321
default-timers ... 322
default-vlan-id ... 323
delay-notifications ... 324
delete-all ... 325
deploy ... 326
dhcp-default-router ... 328
dhcp-gateway-list ... 329
dhcp snooping client-learning disable ... 330
dhcp snooping relay information option subscriber-id ... 331

dhcp snooping trust ... 332
dhcp6 snooping trust ... 333
diagnostics (MRP) ... 334
disable-aging ... 335
disable (LAG) ... 336
disable (NTP) ... 337
disable (Port) ... 338
disable (VSRP) ... 339
disable authentication md5 ... 340
distance (BGP) ... 341
dlb-internal-trunk-hash ... 342
dns-filter ... 344
domain-name ... 346
dot1x auth-fail-action restricted-vlan ... 347
dot1x auth-filter ... 348
dot1x auth-timeout-action ... 350
dot1x disable-filter-strict-security ... 352
dot1x enable ... 353
dot1x guest-vlan ... 355
dot1x initialize ... 356
dot1x max-reauth-req ... 357
dot1x max-req ... 358
dot1x-mka-enable ... 359
dot1x port-control ... 360
dot1x re-authenticate ... 362
dot1x re-auth-timeout-success ... 363
dot1x timeout ... 364
dot1x-enable ... 366
dual-mode ... 367
dynamic ... 369
eee ... 371
egress-buffer-profile ... 373
enable (802.1X authentication) ... 375
enable aaa console ... 377
enable-accounting ... 378
enable acl-per-port-per-vlan ... 379
enable egress-acl-on-control-traffic ... 380
enable (GVRP) ... 381
enable (LAG) ... 383
enable (MRP) ... 384
enable-mka ... 385
enable (Port) ... 386
enable (MAC Port Security) ... 387
enable nd hop-limit ... 388
enable password-display ... 389
enable password-min-length ... 390
enable port-config-password ... 391
enable read-only-password ... 392
enable snmp ... 393
enable strict-password-enforcement ... 394

enable super-user-password ... 395
enable telnet ... 396
enable user ... 397
enable (VSRP) ... 399
enable (Web Authentication) ... 400
enforce-first-as ... 401
erase flash ... 402
erase startup-config ... 403
errdisable packet-inerror-detect ... 404
errdisable recovery ... 405
ethernet (EFM-OAM) ... 408
ethernet loopback ... 410
ethernet loopback (VLAN-aware) ... 412
ethernet loopback test-mac ... 414
excluded-address ... 416
exclude ethernet ... 417

Commands F - J ... 419

failover ... 419
fast-external-fallover ... 421
fast port-span ... 422
fast uplink-span ... 424
fdp advertise ... 426
fdp enable ... 427
fdp holdtime ... 428
fdp run ... 429
fdp timer ... 430
filter-strict-security enable ... 431
fitrace modules flexauth submodule ... 433
flash ... 435
flash-timeout ... 437
flow-control ... 438
force-up ethernet ... 440
format disk0 ... 441
gig-default ... 442
global-filter-strict-security ... 443
graceful-restart (BGP) ... 444
graft-retransmit-timer ... 447
group-router-interface ... 448
gvrp-base-vlan-id ... 449
gvrp-enable ... 450
gvrp-max-leaveall-timer ... 451
hardware-drop-disable ... 452
hello-interval ... 453
hello-timer ... 455
hitless-failover enable ... 456
hitless-reload ... 457
hold-down-interval ... 458
host-max-num ... 459
hostname ... 460
ignore-temp-shutdown ... 461

import-users ... 462
inactivity-timer ... 463
include-port ... 464
initial-ttl ... 465
inline power ... 466
inline power adjust class ... 469
inline power budget ... 471
inline power install-firmware ... 472
inline power install-firmware scp ... 473
inline power interface-mode-2pair-pse ... 475
inline power non-pd-detection enable ... 477
interface ethernet ... 479
interface group-ve ... 480
interface tunnel ... 481
ip access-group ... 482
ip access-list ... 484
ip add-host-route-first ... 485
ip address ... 486
ip-address (VSRP) ... 487
ip arp inspection validate ... 488
ip arp inspection syslog disable ... 490
ip arp inspection vlan ... 491
ip bootp-gateway ... 492
ip bootp-use-intf-ip ... 493
ip dhcp-client auto-update enable ... 494
ip dhcp-client enable ... 495
ip dhcp-client continuous-mode max-duration ... 496
ip dhcp-client discover-interval ... 497
ip dhcp-server arp-ping-timeout ... 498
ip dhcp-server enable ... 499
ip dhcp-server mgmt ... 500
ip dhcp-server server-identifier ... 501
ip dhcp-server pool ... 502
ip dhcp-server relay-agent-echo enable ... 503
ip dhcp snooping vlan ... 504
ip dhcp relay information policy ... 505
ip directed-broadcast ... 506
ip dns ... 507
ip dscp-remark ... 508
ip follow-ingress-vrf ... 509
ipg ... 510
ipg-gmii ... 511
ipg-mii ... 512
ipg-xgmii ... 513
ip helper-use-responder-ip ... 514
ip hitless-route-purge-timer ... 515
ip icmp burst-normal ... 516
ip icmp echo broadcast-request ... 518
ip icmp redirects ... 519
ip icmp unreachable ... 520

ip igmp group-membership-time 522
ip igmp max-response-time 523
ip igmp port-version 524
ip igmp proxy 525
ip igmp query-interval 527
ip igmp tracking 528
ip igmp version 529
ip max-mroute 530
ip mroute 531
ip mroute (next hop) 533
ip mroute next-hop-enable-default 535
ip mroute next-hop-recursion 536
ip multicast 538
ip multicast age-interval 540
ip multicast disable-flooding 541
ip multicast leave-wait-time 542
ip multicast max-response-time 543
ip multicast mcache-age 544
ip multicast query-interval 545
ip multicast report-control 546
ip multicast verbose-off 547
ip multicast version 548
ip multicast-routing rpf-check mac-movement 549
ip multicast-nonstop-routing 550
ip pcp-remark 551
ip pim 552
ip pim border 554
ip pim dr-priority 555
ip pim neighbor-filter 556
ip pimsm-snooping 558
ip pim-sparse 559
ip policy route-map 560
ip preserve-acl-user-input-format 561
ip-proto 562
ip radius source-interface 563
ip router-id 565
ip show-portname 566
ip show-service-number-in-log 567
ip ssh authentication-retries 568
ip ssh client 569
ip ssh encryption aes-only 571
ip ssh encryption disable-aes-cbc 572
ip ssh idle-time 573
ip ssh interactive-authentication 574
ip ssh key-authentication 575
ip ssh key-exchange-method dh-group14-sha1 576
ip ssh password-authentication 577
ip ssh permit-empty-password 578
ip ssh port 579
ip ssh pub-key-file 580

ip ssh scp ... 582
ip ssh strict-management-vrf ... 583
ip ssh timeout ... 584
ip ssl ... 585
ip ssl min-version ... 588
ip-subnet ... 589
ip syslog source-interface ... 590
ip tacacs source-interface ... 592
ip tcp burst-normal ... 594
ip tcp keepalive ... 596
ip tftp source-interface ... 597
ip use-acl-on-arp ... 599
ipv6 access-list ... 601
ipv6 address ... 602
ipv6 cache-lifetime ... 603
ipv6 dhcp-relay destination ... 604
ipv6 dhcp-relay distance ... 605
ipv6 dhcp-relay include-options ... 606
ipv6 dhcp-relay maximum-delegated-prefixes ... 607
ipv6 dhcp6 snooping ... 609
ipv6 enable ... 610
ipv6 hitless-route-purge-timer ... 611
ipv6 load-sharing ... 612
ipv6 max-mroute ... 613
ipv6 mld group-membership-time ... 614
ipv6 mld llqi ... 615
ipv6 mld max-group-address ... 616
ipv6 mld max-response-time ... 617
ipv6 mld port-version ... 618
ipv6 mld query-interval ... 619
ipv6 mld robustness ... 620
ipv6 mld static-group ... 621
ipv6 mld tracking ... 623
ipv6 mroute ... 624
ipv6 mroute (next hop) ... 626
ipv6 mroute next-hop-enable-default ... 628
ipv6 mroute next-hop-recursion ... 629
ipv6 multicast age-interval ... 631
ipv6 multicast disable-flooding ... 632
ipv6 multicast leave-wait-time ... 633
ipv6 multicast mcache-age ... 634
ipv6 multicast query-interval ... 635
ipv6 multicast report-control ... 636
ipv6 multicast verbose-off ... 637
ipv6 multicast version ... 638
ipv6 multicast-boundary ... 639
ipv6 multicast-routing rpf-check mac-movement ... 640
ipv6 nd router-preference ... 641
ipv6 nd skip-interface-ra ... 642
ipv6 neighbor inspection ... 643

ipv6 neighbor inspection vlan ... 645
ipv6 pim border ... 646
ipv6 pim dr-priority ... 647
ipv6 pim neighbor-filter ... 648
ipv6 pim-sparse ... 650
ipv6-proto ... 651
ipv6 raguard policy ... 652
ipv6 raguard vlan ... 653
ipv6 raguard whitelist ... 654
ipv6 route ... 655
ipv6 router pim ... 657
ipv6 traffic-filter ... 658
ipv6-address auto-gen-link-local ... 659
ipv6-neighbor inspection trust ... 660
ipv6 unicast-routing ... 661
ipx-network ... 662
ipx-proto ... 664
jitc enable ... 665
jitc show ... 666
join-timer leave-timer leaveall-timer ... 667
jumbo ... 669

Commands K - S ... 671

keep-alive-vlan ... 671
key-server-priority ... 673
kill ... 674
lacp-timeout ... 675
lag ... 676
lease ... 678
legacy-inline-power ... 679
link-config gig copper autoneg-control ... 680
link-error-disable ... 682
link-fault-signal ... 684
link-keepalive ethernet ... 685
link-keepalive interval ... 687
link-keepalive retries ... 688
link-oam ... 689
lldp advertise link-aggregation ... 690
lldp advertise mac-phy-config-status ... 691
lldp advertise management-address ... 693
lldp advertise max-frame-size ... 695
lldp advertise med-capabilities ... 697
lldp advertise med-power-via-mdi ... 698
lldp advertise port-description ... 700
lldp advertise port-vlan-id ... 701
lldp advertise power-via-mdi ... 702
lldp advertise system-capabilities ... 704
lldp advertise system-description ... 705
lldp advertise system-name ... 706
lldp enable ports ... 707
lldp enable receive ... 708

lldp enable snmp med-topo-change-notifications 710
lldp enable snmp notifications 711
lldp enable transmit 712
lldp max-neighbors-per-port 713
lldp max-total-neighbors 714
lldp med fast-start-repeat-count 715
lldp med location-id civic-address 716
lldp med location-id coordinate-based 720
lldp med location-id ecs-elin 722
lldp med network-policy application 723
lldp reinit-delay 726
lldp run 727
lldp snmp-notification-interval 728
lldp tagged-packets 729
lldp transmit-delay 730
lldp transmit-hold 731
lldp transmit-interval 732
lldp-pass-through 733
load-balance symmetric 734
local-as 735
local-userdb 736
logging 737
logging buffered 738
logging console 740
logging cli-command 741
logging-enable 742
logging enable config-changed 743
logging enable rfc5424 744
logging enable user-login 745
logging facility 746
logging host 748
logging on 749
logging persistence 750
login-page 751
loop-detection 752
loop-detection-interval 753
loop-detection shutdown-disable 754
loop-detection-syslog-interval 755
mac-age-time 756
mac-authentication apply-mac-auth-filter 757
mac-authentication auth-fail-action 758
mac-authentication auth-fail-dot1x-override 760
mac-authentication auth-fail-vlan-id 761
mac-authentication auth-filter 762
mac-authentication auth-passwd-format 763
mac-authentication auth-timeout-action 765
mac-authentication clear-mac-session 767
mac-authentication disable-aging 768
mac-authentication disable-ingress-filtering 770
mac-authentication dos-protection 771

mac-authentication dot1x-override ... 773
mac-authentication enable ... 774
mac-authentication enable (Flexible authentication) ... 776
mac-authentication enable-dynamic-vlan ... 778
mac-authentication hw-deny-age ... 779
mac-authentication max-accepted-session ... 780
mac-authentication max-age ... 781
mac-authentication move-back-to-old-vlan ... 782
mac-authentication no-override-restrict-vlan ... 784
mac-authentication password-format ... 786
mac-authentication mac-filter ... 788
mac-authentication password-override ... 789
mac-authentication password-override (Flexible authentication) ... 790
mac-authentication save-dynamicvlan-to-config ... 791
mac filter ... 792
mac filter enable-accounting ... 794
mac filter-group ... 795
mac filter-group log-enable ... 796
mac filter log-enable ... 797
mac-learn-disable ... 798
mac-notification interval ... 799
mac-movement notification ... 800
macsec cipher-suite ... 801
macsec confidentiality-offset ... 803
macsec frame-validation ... 804
macsec replay-protection ... 806
mac-session-aging max-age ... 808
mac-session-aging no-aging ... 809
management-vlan ... 810
management-vrf ... 811
master ... 812
master (MRP) ... 813
master-vlan ... 814
master-vlan (STP) ... 815
match as-path ... 816
match community ... 817
match interface ... 818
match ip address ... 819
match ipv6 address ... 820
match metric ... 821
match protocol ... 822
match route-type ... 823
match tag ... 824
maximum (Port Security) ... 825
maximum-paths ... 826
maximum-paths ebgp ibgp ... 828
maximum-preference ... 830
maxreq ... 831
max-hw-age ... 832
max-mcache ... 833

max-sw-age 834
med-missing-as-worst 835
member-group 836
member-group (STP) 837
member-vlan 838
member-vlan (STP) 839
mesh-group 840
message-interval 841
metric-type 842
metro-ring 843
metro-rings 844
mdi-mdix 845
mirror-port 847
mka-cfg-group 848
monitor (LAG) 850
monitor 852
mount disk0 854
mstp admin-edge-port 855
mstp admin-pt2pt-mac 856
mstp disable 857
mstp edge-port-auto-detect 858
mstp force-migration-check 859
mstp force-version 860
mstp forward-delay 861
mstp hello-time 862
mstp instance 863
mstp max-age 865
mstp max-hops 866
mstp name 867
mstp revision 868
mstp scope 869
mstp start 870
multicast disable-pimsm-snoop 871
multicast fast-convergence 872
multicast fast-leave-v2 873
multicast limit 874
multicast pimsm-snooping prune-wait 876
multicast port-version 877
multicast proxy-off 878
multicast router-port 879
multicast static-group 881
multicast tracking 883
multicast version 884
multicast6 disable-mld-snoop 885
multicast6 disable-pimsm-snoop 886
multicast6 fast-convergence 887
multicast6 port-version 888
multicast6 proxy-off 889
multicast6 router-port 890
multicast6 static-group 891

multicast6 tracking 893
multicast6 version 894
multipath 895
name (MRP) 897
nbr-timeout 898
neighbor activate 899
neighbor advertisement-interval 901
neighbor allowas-in 903
neighbor as-override 904
neighbor capability as4 905
neighbor capability orf prefixlist 906
neighbor default-originate 908
neighbor description 909
neighbor ebgp-btsh 911
neighbor ebgp-multihop 912
neighbor enforce-first-as 914
neighbor filter-list 915
neighbor local-as 917
neighbor maxas-limit in 918
neighbor maximum-prefix 920
neighbor next-hop-self 921
neighbor password 923
neighbor peer-group 925
neighbor prefix-list 927
neighbor remote-as 929
neighbor remove-private-as 931
neighbor route-map 933
neighbor route-reflector-client 934
neighbor send-community 935
neighbor shutdown 937
neighbor soft-reconfiguration inbound 939
neighbor timers 941
neighbor update-source 943
neighbor weight 945
netbios-name-server 946
netbios-proto 947
network 948
network (dhcp) 950
next-bootstrap-server 951
next-hop-enable-default 952
next-hop-recursion 953
no-dynamic-aging 954
non-preempt-mode 955
ntp 956
ntp-interface 957
openflow controller 958
openflow default send-to-controller 960
openflow enable 961
openflow hello-reply disable 963
openflow log timeout 964

openflow protected-vlans ... 965
openflow purge-time ... 966
optical-monitor ... 967
option ... 969
originator-id ... 971
other-proto ... 972
packet-inerror-detect ... 973
pass-through ... 974
peer ... 975
peer disable-fast-failover ... 977
peer rbridge-id ... 978
peer timers ... 979
peer-info ... 980
pdu-rate (EFM-OAM) ... 981
phy cable diagnostics tdr ... 982
phy-fifo-depth ... 983
ping ... 984
port-name ... 986
port-name (LAG) ... 987
port security ... 988
port-down-authenticated-mac-cleanup ... 989
port-down-disable-laser ... 990
ports ... 991
port-statistics-reset-timestamp enable ... 993
prefix-list ... 994
preforwarding-time ... 995
pre-shared-key ... 996
primary-port ... 998
priority ... 999
priority-flow-control ... 1000
priority-flow-control enable ... 1002
priority ignore-8021p ... 1004
privilege ... 1005
profile-config ... 1007
protected-link-group ... 1009
prune-timer ... 1011
prune-wait ... 1012
pvlan mapping ... 1013
pvlan pvlan-trunk ... 1014
pvlan type ... 1015
pvst-mode ... 1017
pvstplus-protect ... 1018
qd ... 1020
qd-buffer ... 1022
qd-buffer-profile ... 1023
qd-descriptor ... 1024
qd-share-level ... 1025
qos egress-buffer-profile ... 1026
qos ingress-buffer-profile ... 1029
qos-internal-trunk-queue ... 1031

qos mechanism 1033
qos name 1034
qos priority-to-pg 1035
qos profile 1037
qos scheduler-profile 1039
qos tagged-priority 1042
qos-tos map dscp-priority 1043
radius-client coa host 1045
radius-client coa port 1046
rp-embedded 1047
radius-server enable 1048
radius-server host 1049
radius-server key 1052
radius-server retransmit 1053
radius-server timeout 1054
raguard 1055
rate-limit input 1056
rate-limit output 1057
rate-limit-log 1058
rbridge-id 1059
rconsole 1060
rd 1061
re-authentication (802.1x authentication) 1062
re-authentication (Flexible authentication) 1063
reauth-period 1064
reauth-time 1065
redistribute ospf 1066
redistribute (BGP) 1068
register-probe-time 1070
register-suppress-time 1071
relative-utilization 1072
remark 1074
remote-loopback 1076
reserved-vlan-map 1078
restart-ports 1079
restart-vsrp-port 1080
restricted-vlan 1081
reverse-path-check 1082
ring-interface 1084
rmon alarm 1085
rmon event 1087
rmon history 1089
route-precedence 1091
route-precedence admin-distance 1093
router bgp 1094
router-interface 1095
router msdp 1096
route-only 1097
router pim 1099
router vsrp 1101

rpf-mode ... 1102
rp-address ... 1104
rp-adv-interval ... 1106
rp-candidate ... 1107
save-current-values ... 1109
save-dynamicvlan-to-config ... 1110
server (NTP) ... 1111
servertimeout ... 1112
scale-timer ... 1113
scheduler-profile ... 1114
set-active-mgmt ... 1115
set ip next-hop ... 1116
sflow agent-ip ... 1118
sflow destination ... 1119
sflow enable ... 1121
sflow export ... 1122
sflow forwarding ... 1123
sflow forwarding (LAG) ... 1124
sflow management-vrf-disable ... 1125
sflow max-packet-size ... 1126
sflow polling-interval ... 1127
sflow sample ... 1128
sflow sample-mode ... 1130
sflow source ... 1131
sflow source-port ... 1133
sflow version ... 1134
short-path-forwarding ... 1135

Show Commands ... 1137
show 802-1w ... 1137
show aaa ... 1139
show access-list ... 1141
show access-list accounting ... 1143
show acl-on-arp ... 1147
show arp ... 1148
show auth-mac-addresses ... 1149
show boot-preference ... 1154
show breakout ... 1155
show cable-diagnostics tdr ... 1157
show captive-portal ... 1159
show chassis ... 1161
show cluster ccp ... 1163
show cluster client ... 1165
show cluster config ... 1167
show configuration ... 1168
show cpu ... 1169
show cpu histogram ... 1171
show default values ... 1176
show dir ... 1177
show dlb-internal-trunk-hash ... 1178
show dot1x ... 1179

show dot1x configuration ... 1181
show dot1x mac-address-filter ... 1184
show dot1x mac-filter ... 1185
show dot1x mac-session ... 1186
show dot1x sessions ... 1188
show dot1x statistics ... 1190
show dot1x-mka config ... 1192
show dot1x-mka config-group ... 1194
show dot1x-mka sessions ... 1196
show dot1x-mka statistics ... 1199
show eee-statistics ... 1201
show eee-statistics ethernet ... 1203
show errdisable ... 1204
show ethernet loopback interfaces ... 1206
show ethernet loopback resources ... 1208
show fdp entry ... 1209
show fdp interface ... 1211
show fdp neighbors ... 1212
show fdp traffic ... 1214
show files ... 1215
show files disk0 ... 1216
show flash ... 1217
show gvrp ... 1218
show gvrp ethernet ... 1220
show gvrp statistics ... 1222
show gvrp vlan ... 1224
show ignore-temp-shutdown ... 1226
show inline power ... 1227
show interfaces ethernet ... 1233
show interfaces tunnel ... 1236
show interfaces ve ... 1238
show ip access-lists ... 1239
show ip client-pub-key ... 1240
show ipc_stats ... 1241
show ip dhcp-server address-pool ... 1242
show ip dhcp-server binding ... 1244
show ip dhcp-server flash ... 1245
show ip dhcp-server summary ... 1246
show ip dhcp snooping flash ... 1247
show ip dhcp snooping info ... 1248
show ip dhcp snooping vlan ... 1250
show ip interface ve ... 1251
show interfaces lag ... 1252
show interfaces stack-ports ... 1255
show ip bgp neighbors ... 1257
show ip bgp summary ... 1259
show ip mroute ... 1262
show ip msdp mesh-group ... 1264
show ip multicast group ... 1266
show ip multicast mcache ... 1268

show ip multicast optimization 1270
show ip multicast pimsm-snooping..... 1271
show ip multicast vlan..... 1272
show ip ospf interface 1278
show ip pim interface..... 1282
show ip pim mcache..... 1283
show ip pim neighbor..... 1289
show ip pim traffic..... 1291
show ip pimsm-snooping cache..... 1294
show ip reverse-path-check..... 1296
show ip reverse-path-check interface..... 1297
show ip source-guard..... 1298
show ip ssh..... 1299
show ip ssl..... 1301
show ip static-arp..... 1302
show ip static mroute..... 1303
show ipv6..... 1304
show ipv6 access-list..... 1305
show ipv6 bgp neighbors..... 1307
show ipv6 bgp summary..... 1308
show ipv6 dhcp-relay..... 1311
show ipv6 dhcp-relay delegated-prefixes..... 1312
show ipv6 dhcp-relay destinations..... 1313
show ipv6 dhcp-relay interface..... 1314
show ipv6 dhcp-relay options..... 1315
show ipv6 dhcp-relay prefix-delegation-information..... 1316
show ipv6 dhcp6 snooping vlan..... 1317
show ipv6 dhcp6 snooping info..... 1318
show ipv6 mroute..... 1319
show ipv6 multicast mcache..... 1321
show ipv6 multicast group..... 1322
show ipv6 multicast mcache..... 1324
show ipv6 multicast optimization 1325
show ipv6 multicast pimsm-snooping..... 1326
show ipv6 multicast vlan..... 1327
show ipv6 ospf interface 1329
show ipv6 neighbor 1334
show ipv6 pim interface..... 1337
show ipv6 pim traffic..... 1338
show ipv6 pimsm-snooping cache..... 1340
show ipv6 raguard 1342
show ipv6 static mroute..... 1344
show ipv6 tunnel..... 1345
show lag..... 1346
show link-error-disable..... 1352
show link-keepalive..... 1354
show link-oam info..... 1356
show link-oam statistics..... 1360
show lldp..... 1364
show lldp local-info..... 1365

show lldp neighbors ... 1368
show lldp statistics ... 1370
show local-userdb ... 1372
show logging ... 1373
show loop-detection resource ... 1375
show loop-detection status ... 1376
show loop-detect no-shutdown-status ... 1377
show mac-address ... 1378
show mac-address cluster ... 1380
show mac-address mdb ... 1382
show mac-authentication configuration ... 1383
show mac-authentication ip-acl ... 1386
show mac-authentication sessions ... 1387
show mac-authentication statistics ... 1389
show macsec statistics ethernet ... 1391
show management-vrf ... 1395
show media ... 1397
show memory ... 1400
show memory task ... 1403
show metro-ring ... 1405
show mirror ... 1408
show monitor ... 1409
show module ... 1410
show mstp ... 1411
show notification-mac ... 1414
show notification mac-movement ... 1415
show ntp associations ... 1417
show ntp status ... 1420
show openflow ... 1422
show openflow controller ... 1424
show openflow datapath-id ... 1425
show openflow flows ... 1426
show openflow groups ... 1428
show openflow interface ... 1430
show openflow meters ... 1431
show optic ... 1433
show packet-inerror-detect ... 1435
show port security ... 1436
show power-savings-statistics ... 1439
show priority-flow-control ... 1441
show protected-link-group ... 1442
show pvlan ... 1443
show pvstplus-protect-ports ... 1444
show qd-buffer-profile ... 1445
show qos egress-buffer-profile ... 1447
show qos ingress-buffer-profile ... 1448
show qos-internal-trunk-queue ... 1449
show qos priority-to-pg ... 1450
show qos-profiles ... 1452
show qos-tos ... 1454

show qos scheduler-profile 1455
show rate-limit broadcast 1458
show rate-limit input 1459
show rate-limit output-shaping 1460
show rate-limit unknown-unicast 1461
show relative-utilization 1462
show reserved-vlan-map 1463
show rmon 1464
show rmon statistics 1469
show running interface 1472
show running-config 1474
show running-config interface ethernet 1476
show running-config interface tunnel 1477
show running-config interface ve 1478
show scheduler-profile 1479
show sflow 1480
show snmp 1482
show span 1485
show span designated-protect 1489
show stack 1490
show stack connection 1492
show stack detail 1494
show stack failover 1496
show stack flash 1497
show stack link-sync 1498
show stack neighbors 1499
show stack rel-ipc stats 1501
show stack resource 1508
show stack stack-ports 1509
show statistics 1511
show statistics dos-attack 1516
show statistics stack-ports 1517
show statistics traffic-policy 1518
show stp-bpdu-guard 1520
show stp-group 1521
show stp-protect-ports 1522
show symmetric-flow-control 1523
show telnet 1524
show topology-group 1526
show traffic-policy 1528
show transmit-counter 1530
show users 1532
show version 1533
show vlan 1536
show vlan-group 1538
show voice-vlan 1539
show vrf 1540
show vsrp 1542
show webauth 1545
show who 1549

Commands Sn - Z **1551**
snmp-client 1551
snmp-server community 1552
snmp-server contact 1554
snmp-server disable 1555
snmp-server enable 1557
snmp-server enable mib 1558
snmp-server enable traps 1559
snmp-server enable traps holddown-time 1561
snmp-server enable traps mac-notification 1562
snmp-server engineid local 1563
snmp-server group 1565
snmp-server host 1567
snmp-server legacy 1569
snmp-server location 1570
snmp-server max-ifindex-per-module 1571
snmp-server preserve-statistics 1572
snmp-server pw-check 1573
snmp-server trap-source 1574
snmp-server user 1575
snmp-server view 1577
source-interface 1579
spanning-tree 1580
spanning-tree 802-1w 1582
spanning-tree 802-1w ethernet 1584
spanning-tree ethernet 1586
spanning-tree designated-protect 1588
spanning-tree root-protect 1589
spanning-tree rstp 1590
speed-duplex 1591
ssh 1593
ssh access-group 1595
stack disable 1596
stack enable 1597
stack mac 1598
stack-port 1600
stack secure-setup 1601
stack stack-port-resiliency 1602
stack suggested-id 1604
stack suppress-warning 1605
stack switch-over 1606
stack-trunk 1607
stack unconfigure 1608
static ethernet 1612
static-mac-address 1613
static-mac-ip-mapping 1615
store-and-forward 1616
stp-bpdu-guard 1618
stp-group 1619
stp-protect 1620

supptimeout....1621
switch-over-active-role....1622
symmetrical-flow-control enable....1623
symmetric-flow-control enable....1625
symmetric-flow-control set....1626
system-max hw-traffic-conditioner....1628
system-max igmp-snoop-group-addr....1629
system-max igmp-snoop-mcache....1630
system-max ip-route....1631
system-max ip-subnet-port....1632
system-max mac....1633
system-max mac-notification-buffer....1634
system-max max-ecmp....1635
system-max mld-snoop-group-addr....1637
system-max mld-snoop-mcache....1638
system-max openflow-flow-entries....1639
system-max openflow-pvlan-entries....1640
system-max openflow-unprotectedvlan-entries....1641
system-max rmon-entries....1642
system-max spanning-tree....1643
system-max view....1644
system-max virtual-interface....1645
system-max vlan....1646
tacacs-server deadtime....1647
tacacs-server enable....1648
tacacs-server host....1649
tacacs-server key....1651
tacacs-server retransmit....1652
tacacs-server timeout....1653
tagged ethernet....1654
tag-profile....1655
tag-profile enable....1656
tag-type....1657
telnet access-group....1659
telnet client....1660
telnet login-retries....1661
telnet login-timeout....1662
telnet server enable....1663
telnet server suppress-reject-message....1664
telnet timeout....1665
terminal monitor....1666
tftp client enable....1667
tftp disable....1668
tftp-server....1669
table-map 1670
timers (BGP)....1672
timeout (EFM-OAM)....1673
timeout quiet-period....1674
timeout re-authperiod....1675
timeout restrict-fwd-period....1676

timeout tx-period ... 1677
topology-group ... 1678
traceroute ... 1679
track-port (VSRP) ... 1681
traffic-policy count ... 1683
traffic-policy rate-limit adaptive ... 1684
traffic-policy rate-limit fixed ... 1686
transmit-counter ... 1688
trunk-threshold ... 1690
trust dscp ... 1691
trust-port ... 1692
tunnel destination ... 1693
tunnel mode gre ip ... 1694
tunnel mode ipv6ip ... 1695
tunnel source ... 1696
unknown-unicast limit ... 1698
unmount disk0 ... 1700
untagged ... 1701
update-lag-name ... 1702
update-time (BGP) ... 1703
uplink-switch ... 1705
use-radius-server ... 1706
username ... 1707
username (Local database) ... 1709
use-v2-checksum ... 1710
use-vrrp-path (RIP) ... 1711
vendor-class ... 1712
verify ... 1713
version ... 1715
violation ... 1717
virtual-ip ... 1719
virtual-port ... 1720
vlan ... 1721
vlan-group ... 1723
voice-vlan ... 1724
vrf ... 1725
vsrp ... 1726
vsrp-aware ... 1728
web access-group ... 1730
web client ... 1731
webauth ... 1732
webauth-redirect-address ... 1733
web-management ... 1734
webpage custom-text ... 1737
webpage logo ... 1739
webpage terms ... 1741
write terminal ... 1742
xwindow-manager ... 1744

Preface

- Contacting RUCKUS Customer Services and Support 29
- Document Feedback 30
- RUCKUS Product Documentation Resources 30
- Online Training Resources 30
- Document Conventions 31
- Command Syntax Conventions 31

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

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

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety 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 some information that you must read before continuing with the current action or task.



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.

Command Syntax Conventions

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

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

About This Document

- New in This Document..... 33
- Supported hardware and software.....33

New in This Document

Information has been added or updated to reflect new FastIron features or enhancements to existing FastIron features.

For commands introduced since Release 08.0.01, a history table provides information on modifications to the command. For commands introduced prior to Release 08.0.01, a history table is not provided, unless the command has been modified in recent releases.

NOTE
In addition to commands that are new or modified for this release, numerous commands for existing FastIron features have been added that were previously described only in FastIron configuration guides.

Modified commands for FastIron 08.0.30p

The following commands have been modified.

- **accept-mode**
- **enable nd hop-limit**
- **inline power install-firmware**
- **inline power install-firmware scp**
- **priority ignore-8021p** (not supported on ICX 7000 series devices)

TABLE 2 Other Enhancements for FastIron 08.0.30 Revision 22

Feature	Description	Location
Minor editorial updates	Minor editorial updates were made throughout the Command Reference.	All chapters.
Updates to address defects	Minor updates on commands throughout to address defects.	All chapters.

Supported hardware and software

This guide supports the following product families for FastIron release 08.0.30:

- FCX Series
- FastIron X Series (FSX 800 and FSX 1600)
- ICX 6610 Series
- ICX 6430 Series (ICX 6430, ICX 6430-C12)
- ICX 6450 Series (ICX 6450, ICX 6450-C12-PD)
- ICX 6650 Series
- ICX 7250 Series
- ICX 7450 Series

- ICX 7750 Series

  NOTE
  The ICX 6430-C switch supports the same feature set as the ICX 6430 switch unless otherwise noted.

  NOTE
  The ICX 6450-C12-PD switch supports the same feature set as the ICX 6450 switch unless otherwise noted.

For information about the specific models and modules supported in a product family, refer to the hardware installation guide for that product family.

Using the FastIron command-line interface

- Accessing the CLI 35
- Searching and filtering command output 38
- Creating an alias for a CLI command 42
- Specifying stack-unit, slot number, and port number 43

Accessing the CLI

Once an IP address is assigned to a Ruckus device running Layer 2 software or to an interface on the Ruckus device running Layer 3 software, you can access the CLI either through a direct serial connection or through a local or remote Telnet session.

You can initiate a local Telnet or SNMP or SSH connection by attaching a cable to a port and specifying the assigned management station IP address.

Command modes

The FastIron 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 1/1/1
device(config-if-e1000-1/1/1)#
```

Command help

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

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

```
device(config)#?
  aaa                       Define authentication method list
  access-list               Define Access Control List (ACL)
  aggregated-vlan           Support for larger Ethernet frames up to 1536 bytes
  alias                     Configure alias or display configured alias
  all-client                Restrict all remote management to a host
  arp                       Enter a static IP ARP entry
  arp-internal-priority     Set packet priority
  arp-subnet-only           Only learn ARP in the subnet of this device
  authentication            Configure flexible authentication
  banner                    Define a login banner
  batch                     Define a group of commands
  boot                      Set system boot options
  (output truncated)
```

To display a list of commands that start with a specified character, type the character followed by a question mark (?) or a tab.

```
device(config)#e ?
ICX6450-48P Switch(config)#e
  enable                    Password, page-mode and other options
  end                       End Configuration level and go to Privileged level
  errdisable                Set Error Disable Attributions
  exit                      Exit current level
  extern-config-file        Extern configuration file
```

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

```
deviceh(config)#qos ?
  egress-buffer-profile   User defined QoS egress profile
  mechanism               Change mechanism
  name                    Change name
  profile                 Change bandwidth allocation
  scheduler-profile       User defined QoS profile
  tagged-priority         Change tagged frame priority to profile mapping
```

Command completion

Command completion allows you to execute a command by entering a partial string.

> **NOTE**
> Command completion is not supported in the boot loader prompt of ICX 6430 and the ICX 6450 devices.

To complete the spelling of commands or keywords automatically, begin typing the command or keyword and then press Tab. For example, at the CLI command prompt, type te and press Tab. For example, entering **conf t** in privileged EXEC mode auto-completes the keyword and executes the **configure terminal** as shown.

```
device#conf t
  terminal   Configure thru terminal
deviceh#conf terminal
device(config)#
```

If there is more than one command or keyword associated with the characters typed, the CLI displays all choices matching the characters. Type another character to identify the keyword you are looking for.

```
device(config)#show li
  license                 Show software license information
  link-error-disable      Link Debouncing Control
  link-keepalive          Link Layer Keepalive
device(config)#show lic
```

```
  license                  Show software license information
device(config)#show license
```

If you enter an invalid command or partial string that cannot be completed, an error message is displayed.

```
device(config)#shw
Unrecognized command
device(config)#shw
```

Scroll control

By default, the CLI uses a page mode to paginate displays that are longer than 23 lines. The maximum number of lines per page is 23 (line 24 is reserved for printing). Displays that are longer than 23 lines are automatically segmented into pages with 23 lines per page.

If you use the question mark (?) to display a listing of available options in a given mode, the display stops at each 23 line increment and lists your choices for continuing the display.

```
aaa
all-client
appletalk
arp
boot
some lines omitted for brevity...

ipx
lock-address
logging
mac
--More--, next page: Space, next line:
Return key, quit: Control-c
```

Use one of the following scrolling options to display additional information:

- Press the **Space bar** to display the next page (one screen at a time).
- Press the **Return** or **Enter** key to display the next line (one line at a time).
- Press **Ctrl+C** or **Ctrl+Q** to cancel the display.
- Use ths **skip** command in privileged EXEC mode to disable page display mode. Use the **page** command to re-enable page display mode

The following example toggles between page display modes.

```
Brocade#skip
Disable page display mode
Brocade#page
Enable page display mode
```

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 3 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.

TABLE 3 CLI line editing commands (continued)

Ctrl+Key combination	Description
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.
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.

Searching and filtering command output

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

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

The --More-- prompt displays when output extends beyond a single page. At 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. In addition, you can search and filter output from this prompt.

At the --More-- prompt, enter a forward slash (/) followed by a search string. The Ruckus device displays output starting from the first line that contains the search string as shown in the following example. The search feature is 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
  temperature         temperature sensor commands
  terminal            display syslog
  traceroute          TraceRoute to IP node
  undebug             Disable debugging functions (see also 'debug')
  undelete            Undelete flash card files
  whois               WHOIS lookup
  write               Write running configuration to flash or terminal
```

To display lines containing only a specified search string (similar) press the plus key (+) at the --More-- prompt followed by a search string. This option is similar to the **include** option supported with **show** commands.

```
--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, press the minus key (-) at the --More-- prompt followed by a search string. This option is similar to the **exclude** option supported with **show** commands.

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

The filtered results are displayed.

```
filtering...
  temperature         temperature sensor commands
  terminal            display syslog
  traceroute          TraceRoute to IP node
  undebug             Disable debugging functions (see also 'debug')
  undelete            Undelete flash card files
  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. See the next section for information on special characters used with regular expressions.

Searching and filtering show command output

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 a string of characters. You can use special characters to construct complex regular expressions.

Using special characters to construct complex regular expressions

Special characters allow you 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. Supported 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+

TABLE 4 Special characters for regular expressions (continued)

Character	Operation
?	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. 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.

TABLE 4 Special characters for regular expressions (continued)

Character	Operation
|	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 a backslash (\ ) before 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 \*
```

Displaying lines containing a specified string

The following command filters the output of the **show interface** command for port 3/11 to display 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 10.168.1.11/24, 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 to display only the lines that do not contain the word "closed". This command can be used to display open connections to the Ruckus 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 10.168.9.37
        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 to display output starting with the first line that contains the word "SSH". This command can be used to display information about SSH connections to the Ruckus device.

```
device#show who | begin SSH
SSH connections:
 1      established, client ip address 10.168.9.210
        7 seconds in idle
 2      closed
 3      closed
 4      closed
 5      closed
```

Syntax: *show-command* | **begin** *regular-expression*

Creating an alias for a CLI command

An alias serves as a shorthand version of a longer CLI command. For example, you can create an alias called *shoro* for the **show ip route** command. You can then enter te *shoro* alias at the command prompt and the **show ip route** command is issued.

To create an alias called *shoro* for the CLI command **show ip route**, enter the **alias shoro = show ip route** command.

```
device(config)# alias shoro = show ip route
```

Syntax: [no] alias *alias-name* **=** *cli-command*

The *alias-name* must be a single word, without spaces.

After the alias is configured, entering *shoro* in the privileged EXEC mode or in the global configuration mode issues the **show ip route** command.

Enter the command **copy running-config** with the appropriate parameters to create an alias called *wrsbc*.

```
device(config)#alias wrsbc = copy running-config tftp 10.10.10.10 test.cfg
```

To remove the *wrsbc* alias from the configuration, enter one of the following commands.

```
device(config)#no alias wrsbc
```

or

```
device(config)#unalias wrsbc
```

Syntax: unalias *alias-name*

The specified *alias-name* must be the name of an alias already configured on the Ruckus device.

To display the aliases currently configured on the Ruckus device, enter the following command in the Privileged EXEC mode or in the global configuration mode.

```
device# alias
          wrsbc      copy running-config tftp 10.10.10.10 test.cfg
          shoro       show ip route
```

Syntax: alias

Configuration notes for creating a command alias

The following configuration notes apply to this feature:

- You cannot include additional parameters with the alias at the command prompt. For example, after you create the *shoro* alias, *shoro bgp* would not be a valid command.
- If configured on the Ruckus device, authentication, authorization, and accounting is performed on the actual command, not on the alias for the command.
- To save an alias definition to the startup-config file, use the **write memory** command.

Specifying stack-unit, slot number, and port number

Many CLI commands require users to enter port numbers as part of the command syntax, and many **show** command outputs display port numbers. Port numbers are entered and displayed in one of the following formats:

- port number only
- slot number and port number
- stack-unit, slot number, and port number

Not all formats are supported on all devices. To identify a port, refer to the labels on the front panel of the device.

Specifying a port on a modular device

On modular devices such as the FSX 800 and FSX 1600, you must specify the port number in the following format when you issue a command that requires a port parameter: *slot/port*.

The following example enters the ethernet interface sub-configuraton mode for the first port on a modular device.

```
device(config)#interface e 1/1
device(config-if-1/1)#
```

Specifying a port on stackable devices

On stackable devices (FCX and ICX) you must specify the port in the following format when you issue a command that requires a port parameter: *stack-unit /slot/port*.

The following example enters the ethernet interface sub-configuraton mode for the first port on a stackable device.

```
device(config)#interface e 1/1/1
device(config-if-e1000-1/1/1)#
```

Refer to "Brocade Stackable Devices" in the *FastIron Ethernet Switch Stacking Configuration Guide* for more information on stackable devices.

Commands A - E

100-fx

Enables 100Base-FX on chassis-based and stackable devices.

Syntax

100-fx

no 100-fx

Command Default

100Base-FX is not enabled after installation.

Modes

Interface configuration mode

Usage Guidelines

After you physically install a 100Base-FX transceiver, you must use this command to enable 100Base-FX support on the device.

FastIron devices support the following types of SFPs for 100BaseFX:

- *Multimode SFP*—maximum distance is 2 kilometers
- *Long Reach (LR)*—maximum distance is 40 kilometers
- *Intermediate Reach (IR)* —maximum distance is 15 kilometers

For information about supported SFP and SFP+ transceivers on FastIron devices, refer to the *Brocade Optics Family Datasheet* on the Brocade website.

NOTE
You must disable 100Base-FX support before inserting a different type of module in the same port. Otherwise, the device will not recognize traffic traversing the port.

The **no** form of the command disables 100Base-FX support.

Examples

The following example enables support for 100Base-FX on a fiber port.

```
device(config)# interface ethernet 1/1/6
device(config-if-e1000-1/1/6)# 100-fx
```

100-tx

Configures a 1000Base-TX SFP to operate at a speed of 100 Mbps.

Syntax

100-tx

no 100-tx

Command Default

1000Base-TX SFP is not configured to operate at a speed of 100 Mbps.

Modes

Interface configuration mode

Usage Guidelines

This command requires auto negotiation to be enabled on the other end of the link.

Although combo ports (ports 1 - 4) on Hybrid Fiber (HF) models support the 1000Base-TX SFP, they cannot be configured to operate at 100 Mbps. The 100 Mbps operating speed is supported only with non-combo ports (ports 5-24).

The FCX624S-F is the only FCX model that supports the 1000Base-TX SFP module, and only on the non-combo ports (ports 5-24). The FCX624S-F does not have a specific command to enable the 1000Base-TX SFP optic at 100 Mbps. You must manually configure it with the **speed-duplex 100-full** command.

1000Base-TX modules must be configured individually, one interface at a time. 1000Base-TX modules do not support Digital Optical Monitoring. Hotswap is supported for this module when it is configured in 100M mode.

The **no** form of the command disables 1000Base-TX SFP support.

Examples

The following example shows how to configure a 1000Base-TX SFP.

```
device(config)# interface ethernet 1/5/1
device(config-if-e1000-1/5/1)# 100-tx
```

aaa accounting commands

Configures the AAA accounting configuration parameters for EXEC commands.

Syntax

aaa accounting commands *privilege-level* **default start-stop radius** [**tacacs+**] [**none**]

no aaa accounting commands *privilege-level* **default start-stop radius** [**tacacs+**] [**none**]

aaa accounting commands *privilege-level* **default start-stop tacacs+** [**radius**] [**none**]

no aaa accounting commands *privilege-level* **default start-stop tacacs+** [**radius**] [**none**]

aaa accounting commands *privilege-level* **default start-stop none**

no aaa accounting commands *privilege-level* **default start-stop none**

Command Default

AAA accounting is disabled.

Parameters

privilege-level

Configures the device to perform AAA accounting for the commands available at the specified privilege level. Valid values are 0 (Super User level - all commands), 4 (Port Configuration level - port-config and read-only commands), and 5 (Read Only level - read-only commands).

default

Configures the default named list.

start-stop

Configures to send an Accounting Start packet to the AAA accounting server when you enter a command, and an Accounting Stop packet when the service provided by the command is completed.

radius

Configures RADIUS accounting.

tacacs+

Configures TACACS+ accounting.

none

Disables accounting. This is equivalent to using the **no** form of the command.

Modes

Global configuration mode

Usage Guidelines

You can configure AAA accounting for CLI commands by specifying a privilege level whose commands require accounting.

NOTE
If authorization is enabled, and the command requires authorization, then authorization is performed before accounting takes place. If authorization fails for the command, no accounting takes place.

You can configure RADIUS, TACACS+, and None as accounting methods. If the configured primary accounting fails due to an error, the device tries the backup accounting methods in the order they are configured.

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

Examples

The following example shows how to configure the Brocade device to perform RADIUS accounting for the commands available at the Super User privilege level (that is, all commands on the device).

```
device(config)# aaa accounting commands 0 default start-stop radius
```

The following example shows how to configure the Brocade device to perform TACACS+ accounting for the commands available at the Read-only level (that is, read-only commands). The command also configures TACACS+ as the primary accounting followed by RADIUS.

```
device(config)# aaa accounting commands 5 default start-stop tacacs+ radius
```

aaa accounting dot1x

Enables 802.1X accounting.

Syntax

aaa accounting dot1x default start-stop radius [**none**]

no aaa accounting dot1x default start-stop radius [**none**]

aaa accounting dot1x default start-stop none

no aaa accounting dot1x default start-stop none

Command Default

AAA accounting is disabled.

Parameters

default

Configures the default named list.

start-stop

Configures to sent an Accounting Start packet is sent to the RADIUS accounting server when 802.1x session is enabled, and an Accounting Stop packet is sent when the service provided by the command is completed.

radius

Configures RADIUS accounting.

none

Disables accounting. The client is automatically authenticated without the device using information supplied by the client.

Modes

Global configuration mode

Usage Guidelines

You can configure both RADIUS and None as accounting methods. If the configured primary accounting fails due to an error, the device tries the backup accounting methods in the order they are configured.

NOTE
If authorization is enabled, and the command requires authorization, then authorization is performed before accounting takes place. If authorization fails for the command, no accounting takes place.

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

Examples

The following example shows how to enable 802.1x accounting.

```
device(config)# aaa accounting dot1x default start-stop radius
```

The following example shows how to enable 802.1x accounting and configure RADIUS as the primary accounting method. If the configured primary RADIUS accounting fails due to an error, the device tried the backup accounting method "none", that is, accounting will be disabled.

```
device(config)# aaa accounting dot1x default start-stop radius none
```

aaa accounting exec

Configures the AAA accounting configuration parameters for SSH and Telnet access.

Syntax

aaa accounting exec default start-stop radius [**tacacs+**] [**none**]

no aaa accounting exec default start-stop radius [**tacacs+**] [**none**]

aaa accounting exec default start-stop tacacs+ [**radius**] [**none**]

no aaa accounting exec default start-stop tacacs+ [**radius**] [**none**]

aaa accounting exec default start-stop none

no aaa accounting exec default start-stop none

Command Default

AAA accounting is disabled.

Parameters

default
Configures the default named list.

start-stop
Configures to send an Accounting Start packet to the AAA accounting server when an authenticated user establishes a Telnet or SSH session on the Brocade device, and an Accounting Stop packet when the user logs out.

radius
Configures RADIUS accounting.

tacacs+
Configures TACACS+ accounting.

none
Disables accounting.

Modes

Global configuration mode

Usage Guidelines

You can configure RADIUS, TACACS+, and None as accounting methods. If the configured primary accounting fails due to an error, the device tries the backup accounting methods in the order they are configured.

NOTE
If authorization is enabled, and the command requires authorization, then authorization is performed before accounting takes place. If authorization fails for the command, no accounting takes place.

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

Examples

The following example shows how to configure the Brocade device to perform RADIUS accounting for Telnet or SSH access.

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

The following example shows how to configure the Brocade device to perform TACACS+ accounting for Telnet or SSH access and to specify the order of accounting preference.

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

aaa accounting system

Configures AAA accounting to record when system events occur on the device.

Syntax

aaa accounting system default start-stop radius [**tacacs+**] [**none**]

no aaa accounting system default start-stop radius [**tacacs+**] [**none**]

aaa accounting system default start-stop tacacs+ [**radius**] [**none**]

no aaa accounting system default start-stop tacacs+ [**radius**] [**none**]

aaa accounting system default start-stop none

no aaa accounting system default start-stop none

Command Default

AAA accounting is disabled.

Parameters

default
Configures the default named list.

start-stop
Configures to send an Accounting Start packet to be sent to the AAA accounting server when a system event occurs, and an Accounting Stop packet to be sent when the system event is completed.

radius
Configures RADIUS accounting.

tacacs+
Configures TACACS+ accounting.

none
Disables accounting.

Modes

Global configuration mode

Usage Guidelines

You can configure RADIUS, TACACS+, and None as accounting methods. If the configured primary accounting fails due to an error, the device tries the backup accounting methods in the order they are configured.

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

Examples

The following example shows how to configure the Brocade device to perform RADIUS accounting to record when a system event occurs.

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

The following example shows how to configure the device to perform TACACS+ accounting to record when a system event occurs and to specify RADIUS and None as the backup accounting methods.

```
device(config)# aaa accounting system default start-stop tacacs+ radius none
```

aaa authentication dot1x

Enables 802.1X authentication.

Syntax

aaa authentication dot1x default radius [**none**]

no aaa authentication dot1x default radius [**none**]

aaa authentication dot1x default none

no aaa authentication dot1x default none

Command Default

AAA authentication is disabled.

Parameters

default

Configures the default named list.

radius

Configures RADIUS authentication.

none

Disables authentication. The client is automatically authenticated by other means, without the device using information supplied by the client.

Modes

Global configuration mode

Usage Guidelines

To use 802.1X authentication, you must specify an authentication method to be used to authenticate clients. Brocade supports RADIUS authentication with 802.1X authentication. To use RADIUS authentication with 802.1X authentication, you create an authentication method list for 802.1X and specify RADIUS as an authentication method, and then configure communication between the Brocade device and the RADIUS server.

If you specify both **RADIUS** and **none**, make sure **RADIUS** comes before **none** when the command is issued.

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

Examples

The following example shows how to enable 802.1x authentication.

```
device(config)# aaa authentication dot1x default radius
```

aaa authentication enable

Configures the AAA authentication method for securing access to the Privileged EXEC level and global configuration levels of the CLI.

Syntax

aaa authentication enable default *method-list* [*method-list* ...]

no aaa authentication enable default *method-list* [*method-list* ...]

aaa authentication enable implicit-user

no aaa authentication enable implicit-user

Command Default

The AAA authentication method list is not configured.

By default, the device prompts for a username and password.

Parameters

default

Configures the default authentication method list.

method-list

Configures the following authentication methods.

enable

Authenticate using the password you configured for the Super User privilege level. This password is configured using the **enable super-user-password** command.

line

Authenticate using the password you configured for Telnet access. The Telnet password is configured using the **enable telnet password** command.

local

Authenticate using a local username and password you configured on the device. Local usernames and passwords are configured using the **username** command.

none

Does not use any authentication method. The device automatically permits access.

radius

Authenticate using the database on a RADIUS server. You also must identify the server to the device using the **radius-server** command.

tacacs

Authenticate using the database on a TACACS server. You also must identify the server to the device using the **tacacs-server** command.

tacacs+

Authenticate using the database on a TACACS+ server. You also must identify the server to the device using the **tacacs-server** command.

implicit-user

Configures the device to prompt only for a password when a user attempts to gain Super User access to the Privileged EXEC and global configuration levels of the CLI.

Modes

Global configuration mode

Usage Guidelines

You can specify a primary authentication method and up to six backup authentication methods. If the configured primary authentication fails due to an error, the device tries the backup authentication methods in the order they appear in the list.

If enable authentication is configured on the device, when a user attempts to gain Super User access to the Privileged EXEC and global configuration levels of the CLI, by default the device prompts for a username and password. You can configure the device to prompt only for a password. The device uses the username entered at login, if one is available. If no username was entered at login, the device prompts for both username and password.

The **no** form of the command removes authentication method.

Examples

The following example shows how to configure TACACS/TACACS+ as the primary authentication method for securing access to the Privileged EXEC and global configuration levels of the CLI. In this example, TACACS/TACACS+ is configured to be the primary authentication method for securing access. If TACACS/TACACS+ authentication fails due to an error with the server, local authentication is used instead. If local authentication fails, no authentication is used; the device automatically permits access.

```
device(config)# aaa authentication enable default tacacs local none
```

The following example shows how to configure RADIUS as the primary authentication method and other backup authentication methods.

```
device(config)# aaa authentication enable default radius tacacs tacacs+ enable local line none
```

The following example shows how to configure the device to prompt only for a password when a user attempts to gain Super User access to the Privileged EXEC and global configuration levels of the CLI.

```
device(config)# aaa authentication enable implicit-user
```

aaa authentication login

Configures the AAA authentication method for securing access to Telnet or SSH access to the CLI.

Syntax

aaa authentication login default *method-list* [*method-list* ...]

no aaa authentication login default *method-list* [*method-list* ...]

aaa authentication login privilege-mode

no aaa authentication login privilege-mode

Command Default

The AAA authentication method list is not configured.

By default, a user enters the User EXEC mode after a successful login through Telnet or SSH.

Parameters

default

Configures the default authentication method list.

method-list

Configures the following authentication methods.

enable

Authenticate using the password you configured for the Super User privilege level. This password is configured using the **enable super-user-password** command.

line

Authenticate using the password you configured for Telnet access. The Telnet password is configured using the **enable telnet password** command.

local

Authenticate using a local username and password you configured on the device. Local usernames and passwords are configured using the **username** command.

none

Does not use any authentication method. The device automatically permits access.

radius

Authenticate using the database on a RADIUS server. You also must identify the server to the device using the **radius-server** command.

tacacs

Authenticate using the database on a TACACS server. You also must identify the server to the device using the **tacacs-server** command.

tacacs+

Authenticate using the database on a TACACS+ server. You also must identify the server to the device using the **tacacs-server** command.

privilege-mode

Configures the device to enter the privileged EXEC mode after a successful login through Telnet or SSH.

Modes

Global configuration mode

Usage Guidelines

You can specify a primary authentication method and up to six backup authentication methods. If the configured primary authentication fails due to an error, the device tries the backup authentication methods in the order they appear in the list.

By default, a user enters User EXEC mode after a successful login through Telnet or SSH. Optionally, you can configure the device so that a user enters Privileged EXEC mode after a Telnet or SSH login. The user privilege level is based on the privilege level granted during login.

The **no** form of the command removes the authentication method.

Examples

The following example shows how to configure RADIUS as the primary authentication method for securing Telnet access to the CLI. If RADIUS authentication fails due to an error with the server, local authentication is used instead.

```
device(config)# aaa authentication login default radius local
```

The following example shows how to configure RADIUS as the primary authentication method and other backup authentication methods.

```
device(config)# aaa authentication login default radius tacacs tacacs+ enable local line none
```

The following example shows how to configure the device so that a user enters Privileged EXEC mode after a Telnet or SSH login.

```
device(config)# aaa authentication login privilege-mode
```

aaa authentication snmp-server

Configures the AAA authentication method for SNMP server access.

Syntax

aaa authentication snmp-server default *method-list* [*method-list* ...]

no aaa authentication snmp-server default *method-list* [*method-list* ...]

Command Default

The AAA authentication method list is not configured.

Parameters

default

Configures the default authentication method list.

method-list

Configures the following authentication methods.

enable

Authenticate using the password you configured for the Super User privilege level. This password is configured using the **enable super-user-password** command.

line

Authenticate using the password you configured for Telnet access. The Telnet password is configured using the **enable telnet password** command

local

Authenticate using a local username and password you configured on the device. Local usernames and passwords are configured using the **username** command.

none

Does not use any authentication method. The device automatically permits access.

radius

Authenticate using the database on a RADIUS server. You also must identify the server to the device using the **radius-server** command.

tacacs

Authenticate using the database on a TACACS server. You also must identify the server to the device using the **tacacs-server** command.

tacacs+

Authenticate using the database on a TACACS+ server. You also must identify the server to the device using the **tacacs-server** command.

Modes

Global configuration mode

Usage Guidelines

You can specify a primary authentication method and up to six backup authentication methods. If the configured primary authentication fails due to an error, the device tries the backup authentication methods in the order they appear in the list.

When this command is enabled, community string validation is not performed for incoming SNMP v1and v2c packets. This command takes effect as long as the first varbind for SNMP packets is set to one of the following:

- snAgGblPassword=" username password " (for AAA method local)
- snAgGblPassword=" password " (for AAA method line, enable)

NOTE
Certain SNMP objects need additional validation. These objects include but are not limited to: snAgReload, snAgWriteNVRAM, snAgConfigFromNVRAM, snAgImgLoad, snAgCfgLoad, and snAgGblTelnetPassword.

If AAA is set up to check both the username and password, the string contains the username, followed by a space and then the password. If AAA is set up to authenticate with the current Enable or Line password, the string contains the password only. The configuration can be overridden by the **no snmp-server pw-check** command, which disables password checking for SNMP SET requests.

The **no** form of the command removes the authentication method.

Examples

The following example shows how to configure incoming SNMP SET operations to be authenticated using the locally configured usernames and passwords.

```
device(config)# aaa authentication snmp-server default local
```

aaa authentication web-server

Configures the AAA authentication method to access the device through the Web Management Interface.

Syntax

aaa authentication web-server default *method-list* [*method-list* ...]

no aaa authentication web-server default *method-list* [*method-list* ...]

Command Default

The AAA authentication is not configured.

Parameters

default

Configures the default authentication method list.

method-list

Configures the following authentication methods.

enable

Authenticate using the password you configured for the Super User privilege level. This password is configured using the **enable super-user-password** command.

line

Authenticate using the password you configured for Telnet access. The Telnet password is configured using the **enable telnet password** command.

local

Authenticate using a local username and password you configured on the device. Local usernames and passwords are configured using the **username** command.

none

Does not use any authentication method. The device automatically permits access.

radius

Authenticate using the database on a RADIUS server. You also must identify the server to the device using the **radius-server** command.

tacacs

Authenticate using the database on a TACACS server. You also must identify the server to the device using the **tacacs-server** command.

tacacs+

Authenticate using the database on a TACACS+ server. You also must identify the server to the device using the **tacacs-server** command.

Modes

Global configuration mode

Usage Guidelines

You can specify a primary authentication method and up to six backup authentication methods. If the configured primary authentication fails due to an error, the device tries the backup authentication methods in the order they appear in the list.

The **no** form of the command removes authentication method.

Examples

The following example shows how to configure the device to use the local user accounts to authenticate access to the device through the Web Management Interface. If the device does not have a user account that matches the username and password entered by the user, the user is not granted access.

```
device(config)# aaa authentication web-server default local
```

aaa authorization coa enable

Enables RADIUS Change of Authorization (CoA).

Syntax

aaa authorization coa enable

no aaa authorization coa enable

Command Default

RADIUS CoA is not enabled.

Parameters

None

Modes

Global configuration mode

Usage Guidelines

Use this command to enable RADIUS CoA authorization. The no form of the command disables the CoA functionality. A change of authorization request packet can be sent by the Dynamic Authorization Client (DAC) to change the session authorizations on the Network Access Server (NAS). This is used to change the filters, such as Layer 3 ACLs.

Before RFC 5176 when a user or device was authenticated on the RADIUS server, the session could only be ended if the user or device logs out. RFC 5176 addresses this issue by adding two more packet types to the current RADIUS standard: Disconnect Message and Change of Authorization. The Dynamic Authorization Client (DAC) server makes the requests to either delete the previously established sessions or replace the previous configuration or policies. Currently, these new extensions can be used to dynamically terminate or authorize sessions that are authenticated through multi-device-port-authentication or dot1x authentication.

Examples

The following example enables RADIUS CoA.

```
device(config)# aaa authorization coa enable
```

History

Release version	Command history
08.0.20	This command was introduced.

aaa authorization coa ignore

Discards the specified RADIUS Change of Authorization (CoA) messages.

Syntax

aaa authorization coa ignore { **dm-request** | **modify-acl** }

no aaa authorization coa ignore { **dm-request** | **modify-acl** }

Command Default

The default state is maintained and the packets are not discarded.

Parameters

dm-request
Disconnects the message request.

modify-acl
Modifies the access control list.

Modes

Global configuration mode

Usage Guidelines

Use this command to discard the specified RADIUS messages. A CoA request packet can be sent by the Dynamic Authorization Client (DAC) to change the session authorizations on the Network Access Server (NAS). This is used to change the filters, such as Layer 3 ACLs.

Before RFC 5176 when a user or device was authenticated on the RADIUS server, the session could only be ended if the user or device logs out. RFC 5176 addresses this issue by adding two more packet types to the current RADIUS standard: Disconnect Message and Change of Authorization. The Dynamic Authorization Client (DAC) server makes the requests to either delete the previously established sessions or replace the previous configuration or policies. Currently, these new extensions can be used to dynamically terminate or authorize sessions that are authenticated through multi-device-port-authentication or dot1x authentication.

The **no** form of the command honors the dm-request message.

Examples

The following example ignores the disconnect message request.

```
device(config)# aaa authorization coa ignore dm-request
```

History

Release version	Command history
08.0.20	This command was introduced.

aaa authorization commands

Configures the AAA authorization configuration parameters for EXEC commands.

Syntax

aaa authorization commands *privilege-level* **default radius** [**tacacs+**] [**none**]

no aaa authorization commands *privilege-level* **default radius** [**tacacs+**] [**none**]

aaa authorization commands *privilege-level* **default tacacs+** [**radius**] [**none**]

no aaa authorization commands *privilege-level* **default tacacs+** [**radius**] [**none**]

aaa authorization commands *privilege-level* **default none**

no aaa authorization commands *privilege-level* **default none**

Command Default

AAA authorization is not enabled.

Parameters

privilege-level

Configures the device to perform AAA authorization for the commands available at the specified privilege level. Valid values are 0 (Super User level - all commands), 4 (Port Configuration level - port-config and read-only commands), and 5 (Read Only level - read-only commands).

default

Configures the default named list.

radius

Configures RADIUS authorization.

tacacs+

Configures TACACS+ authorization.

none

Disables accounting.

Modes

Global configuration mode

Usage Guidelines

You can configure RADIUS, TACACS+, and None as authorization methods. If the configured primary authorization fails due to an error, the device tries the backup authorization methods in the order they are configured.

When TACACS+ command authorization is enabled, the Brocade device consults a TACACS+ server to get authorization for commands entered by the user.

When RADIUS command authorization is enabled, the Brocade device consults the list of commands supplied by the RADIUS server during authentication to determine whether a user can issue a command that was entered.

> **NOTE**
> TACACS+ and RADIUS command authorization can be performed only for commands entered from Telnet or SSH sessions, or from the console. No authorization is performed for commands entered at the Web Management Interface.

TACACS+ command authorization is not performed for the following commands:

- At all levels: **exit**, **logout**, **end**, and **quit**.
- At the Privileged EXEC level: **enable** or **enable** *text*, where *text* is the password configured for the Super User privilege level.

Because RADIUS command authorization relies on the command list supplied by the RADIUS server during authentication, you cannot perform RADIUS authorization without RADIUS authentication.

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

Examples

The following example shows how to configure RADIUS command authorization for the commands available at the Super User privilege level (that is, all commands on the device).

```
device(config)# aaa authorization commands 0 default radius
```

The following example shows how to configure TACACS+ command authorization for the commands available at the Super User privilege level (that is, all commands on the device).

```
device(config)# aaa authorization commands 0 default tacacs+
```

aaa authorization exec

Determines the user privilege level when users are authenticated.

Syntax

aaa authorization exec default radius [**tacacs+**] [**none**]

no aaa authorization exec default radius [**tacacs+**] [**none**]

aaa authorization exec default tacacs+ [**radius**] [**none**]

no aaa authorization exec default tacacs+ [**radius**] [**none**]

aaa authorization exec default none

no aaa authorization exec default none

Command Default

AAA authorization is not configured.

Parameters

default
Configures the default named list.

radius
Configures RADIUS authorization.

tacacs+
Configures TACACS+ authorization.

none
Disables accounting.

Modes

Global configuration mode

Usage Guidelines

You can configure RADIUS, TACACS+, and None as authorization methods. If the configured primary authorization fails due to an error, the device tries the backup authorization methods in the order they are configured.

When TACACS+ EXEC authorization is performed, the Brocade device consults a TACACS+ server to determine the privilege level of the authenticated user. If the **aaa authorization exec default tacacs+** command exists in the configuration, following successful authentication, the device assigns the user the privilege level specified by the foundry-privilege-level received from the TACACS+ server. If the **aaa authorization exec default tacacs+** command does not exist in the configuration, then the value in the foundry-privilege-level attribute is ignored, and the user is granted Super User access. Also note that in order for the **aaa authorization exec default tacacs+** command to work, either the **aaa authentication enable default tacacs+** command, or the **aaa authentication login privilege-mode** command must also exist in the configuration.

When RADIUS EXEC authorization is performed, the Brocade device consults a RADIUS server to determine the privilege level of the authenticated user. If the **aaa authorization exec default radius** command exists in the configuration, following successful authentication, the device assigns the user the privilege level specified by the foundry-privilege-level attribute received from the RADIUS server. If the **aaa authorization exec default radius** command does not exist in the configuration, then the value in the foundry-privilege-level attribute is ignored, and the user is granted Super User access. Also note that in order for the **aaa authorization exec default radius** command to work, either the **aaa authentication enable default radius** command, or the **aaa authentication login privilege-mode** command must also exist in the configuration.

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

Examples

The following example shows how to configure TACACS+ EXEC authorization.

```
device(config)# aaa authorization exec default tacacs+
```

The following example shows how to configure RADIUS EXEC authorization.

```
device(config)# aaa authorization exec default radius
```

accept-mode

Enables a non-owner master router to respond to ping, traceroute, and Telnet packets destined for the virtual IPv4 or IPv6 address of a VRRP session.

Syntax

accept-mode

no accept-mode

Command Default

A VRRP non-owner master router does not respond to any packet destined for the virtual IPv4 or IPv6 address.

Modes

VRRP configuration mode

Usage Guidelines

The **no** form of this command causes the nonowner master router to not respond to any packet that is destined for the virtual IPv4 or IPv6 address of the VRRP session.

A VRRP nonowner master router does not respond to any packet that is destined for the virtual IPv4 or IPv6 address. This prevents troubleshooting network connections to this router using ping, traceroute, or Telnet. To resolve this, you can use this command to enable the router to respond to ping, traceroute, and Telnet packets destined for the virtual IPv4 or IPv6 address of a VRRP cluster. The router drops all other packets destined for the virtual IPv4 or IPv6 address of the VRRP session.

NOTE
The **accept-mode** command enables the device to respond to ping, traceroute, and Telnet packets, but the device does not respond to SSH packets. When the device acting as the master router is not the IP address owner (the router with the interface whose actual IP address is used as the virtual router's IP address), the master router accepts only the ARP packets sent to the virtual IP address. When accept mode is configured, the master router responds to ping, TELNET, and traceroute packets sent to the virtual IP address even when the master router is not the IP address owner.

Examples

The following example shows the configuration of accept mode on an IPv6 VRRP backup router.

```
Brocade(config)# interface ve 3
Brocade(config-vif-3)# ipv6 vrrp vrid 2
Brocade(config-vif-3-vrid-2)# backup
Brocade(config-vif-3-vrid-2)# advertise backup
Brocade(config-vif-3-vrid-2)# ipv6-address 2001:DB8::1
Brocade(config-vif-3-vrid-2)# accept-mode
Brocade(config-vif-3-vrid-2)# activate
```

History

Release version	Command history
8.0.01	This command was introduced.
8.0.30b	This command was modified to explain that the **accept-mode** command does not enable a response to SSH packets. The usage guidelines were also updated.

access-control vlan

Enables the VLAN containment for NTP.

Syntax

access-control vlan *vlan-id*

no access-control vlan *vlan-id*

Command Default

VLAN containment for NTP is not enabled.

Parameters

vlan *vlan-id*

Specifies the VLAN number.

Modes

NTP configuration mode

Usage Guidelines

The management interface is not part of any VLAN. When configuring the VLAN containment for NTP, it will not use the management interface to send or receive the NTP packets.

When VLAN is configured,

- NTP time servers should be reachable through the interfaces which belong to the configured VLAN. Otherwise, NTP packets are not transmitted. This is applicable to both the unicast and the broadcast server/client.
- NTP broadcast packets are sent only on the interface which belongs to the configured VLAN.
- The received unicast or broadcast NTP packet are dropped if the interface on which packet has been received does not belong to the configured VLAN.

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

Examples

The following example shows how to enable VLAN containment for NTP.

```
device(config)# ntp
device(config-ntp)# access-control vlan 100
```

access-list enable accounting

Enables Access Control List (ACL) accounting for IPv4 numbered ACLs.

Syntax

access-list *number* **enable-accounting**

no access-list *number* **enable-accounting**

Command Default

This option is disabled.

Parameters

number

Defines the IPv4 ACL ID.

enable-accounting

Enables ACL accounting on the specified interface.

Modes

Global configuration mode

Usage Guidelines

This command is only applicable to numbered ACLs.

The **no** form of this command disables ACL accounting for IPv4 numbered ACLs.

Examples

The following example enables ACL accounting for a numbered ACL.

```
device(config)# access-list 10 permit host 10.10.10.1
device(config)# access-list 10 enable-accounting
device(config)# interface ethernet 1/1
device(config-if-1/1)# ip access-group 10 in
```

The following example enables ACL accounting for an extended ACL.

```
device(config)# ip access-list extended 101
device(config-ip-access-list-101)# enable-accounting
```

History

Release version	Command history
08.0.10	This command was introduced.

access-list deny

Configures the switch to deny packets that match a policy in the access list.

Syntax

access-list *acl-num* **deny** { *hostname* [*wildcard*] [**log**] [**mirror**] | *ip-address* [*wildcard*] [**log**] [**mirror**] | **any** [**log**] [**mirror**] | **host** { *hostname* | *hostip* } [**log**] [**mirror**] }

no access-list *acl-num* **deny** { *hostname* [*wildcard*] [**log**] [**mirror**] | *ip-address* [*wildcard*] [**log**] [**mirror**] | **any** [**log**] [**mirror**] | **host** { *hostname* | *hostip* } [**log**] [**mirror**] }

Command Default

Access lists are not configured

Parameters

acl-num
Specifies the access list number. Values are from 1 through 99 for standard ACLs and from 100 through 199 for extended ACLs.

hostname
Specifies the source host name.

wildcard
Specifies the mask value to compare against the host address or source IP address. The wildcard is in dotted-decimal notation (IP address format).

log
Configures the device to generate syslog entries and SNMP traps for inbound packets that are denied by the access policy.

miror
Configures the device to mirror the traffic that matches the entry.

ip-address
Specifies the source IP address.

any
Configures the policy to match on all host addresses.

host
Configures the source host.

hostname
Specifies the host name.

hostip
Specifies the host IP address.

Modes

Global configuration mode

Usage Guidelines

The wildcard is in dotted-decimal notation (IP address format). It is a four-part value, where each part is 8 bits (one byte) separated by dots, and each bit is a one or a zero. Each part is a number ranging from 0 to 255, for example, 0.0.0.255. Zeros in the mask mean the packet source address must match the source IP address . Ones mean any value matches. For example, the source IP adddress and wildcard values 10.157.22.26 0.0.0.255 mean that all hosts in the Class C subnet 10.157.22.x match the policy.

If you prefer to specify the wildcard (mask value) in CIDR format, you can enter a forward (/) after the IP address, and then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of 10.157.22.26 0.0.0.255 as 10.157.22.26/24. The CLI automatically converts the CIDR number into the appropriate ACL mask (where zeros instead of ones are the significant bits) and changes the non-significant portion of the IP address into ones. For example, if you specify 10.157.22.26/24 or 10.157.22.26 0.0.0.255, and then save the changes to the startup-config file, the value appears as 10.157.22.0/24 (if you have enabled display of subnet lengths) or 10.157.22.0 0.0.0.255 in the startup-config file.

If you enable the software to display IP subnet masks in CIDR format, the mask is saved in the file in "/ mask-bits " format. To enable the software to display the CIDR masks, enter the **ip show-subnet-length** command at the global configuration level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

The **no** form of the command removes the access list.

Examples

The following example shows how to configure a standard ACL and apply it to incoming traffic on port 1/1/1.

```
device(config)# access-list 1 deny host 10.157.22.26 log
device(config)# access-list 1 deny 10.157.29.12 log
device(config)# access-list 1 deny host IPHost1 log
device(config)# access-list 1 permit any
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ip access-group 1 in
device(config)# write memory
```

access-list permit

Configures the switch to permit packets that match a policy in the access list.

Syntax

access-list *acl-num* **permit** { *hostname* [*wildcard*] [**log**] [**mirror**] | *ip-address* [*wildcard*] [**log**] [**mirror**] | **any** [**log**] [**mirror**] | **host** { *hostname* | *hostip* } [**log**] [**mirror**] }

no access-list *acl-num* **permit** { *hostname* [*wildcard*] [**log**] [**mirror**] | *ip-address* [*wildcard*] [**log**] [**mirror**] | **any** [**log**] [**mirror**] | **host** { *hostname* | *hostip* } [**log**] [**mirror**] }

Command Default

Access lists are not configured.

Parameters

acl-num

Specifies the access list number. Values are from 1 through 99 for standard ACLs and from 100 through 199 for extended ACLs.

hostname

Specifies the source host name.

wildcard

Specifies the mask value to compare against the host address or source IP address. The wildcard is in dotted-decimal notation (IP address format).

log

Configures the device to generate syslog entries and SNMP traps for inbound packets that are permitted by the access policy.

miror

Configures the device to mirror the traffic that matches the entry.

ip-address

Specifies the source IP address.

any

Configures the policy to match on all host addresses.

host

Configures the source host.

hostname

Specifies the host name.

hostip

Specifies the host IP address.

Modes

Global configuration mode

Usage Guidelines

The wildcard is in dotted-decimal notation (IP address format). It is a four-part value, where each part is 8 bits (one byte) separated by dots, and each bit is a one or a zero. Each part is a number ranging from 0 to 255, for example, 0.0.0.255. Zeros in the mask mean the packet source address must match the source IP address. Ones mean any value matches. For example, the source IP address and wildcard values 10.157.22.26 0.0.0.255 mean that all hosts in the Class C subnet 10.157.22.x match the policy.

If you prefer to specify the wildcard (mask value) in CIDR format, you can enter a forward (/) after the IP address, and then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of 10.157.22.26 0.0.0.255 as 10.157.22.26/24. The CLI automatically converts the CIDR number into the appropriate ACL mask (where zeros instead of ones are the significant bits) and changes the non-significant portion of the IP address into ones. For example, if you specify 10.157.22.26/24 or 10.157.22.26 0.0.0.255, and then save the changes to the startup-config file, the value appears as 10.157.22.0/24 (if you have enabled display of subnet lengths) or 10.157.22.0 0.0.0.255 in the startup-config file.

If you enable the software to display IP subnet masks in CIDR format, the mask is saved in the file in "/ mask-bits " format. To enable the software to display the CIDR masks, enter the **ip show-subnet-length** command at the global configuration level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

The **no** form of the command removes the access list.

Examples

The following example shows how to configure a standard ACL and apply it to incoming traffic on port 1/1/1.

```
device(config)# access-list 1 deny host 10.157.22.26 log
device(config)# access-list 1 deny 10.157.29.12 log
device(config)# access-list 1 deny host IPHost1 log
device(config)# access-list 1 permit any
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ip access-group 1 in
device(config)# write memory
```

access-list remark

Adds a remark to the following access list entry.

Syntax

access-list remark *comment-text*

no access-list remark *comment-text*

Command Default

Access lists are not remarked.

Parameters

comment-text

Specifies the remark for the following access list entry, up to 256 alphanumeric characters.

Modes

Global configuration mode

Usage Guidelines

ACL comment text describes entries in an ACL. The comment text appears in the output of show commands that display ACL information.

The **no** form of the command removes the remark from the access list.

Examples

The following example adds remarks to entries in a numbered ACL.

```
device(config)# access-list 100 remark The following line permits TCP packets
device(config)# access-list 100 permit tcp 192.168.4.40/24 2.2.2.2/24
device(config)# access-list 100 remark The following permits UDP packets
device(config)# access-list 100 permit udp 192.168.2.52/24 2.2.2.2/24
device(config)# access-list 100 deny ip any any
```

accounting

Enables RADIUS accounting for Web Authentication.

Syntax

accounting

no accounting

Command Default

RADIUS accounting for Web Authentication is not enabled.

Modes

Web Authentication configuration mode

Usage Guidelines

When Web Authentication is enabled, you can enable RADIUS accounting to record login (start) and logout (stop) events per host. The information is sent to a RADIUS server.

The **no** form of the command disables RADIUS accounting for Web Authentication.

Examples

The following example enables RADIUS accounting for Web Authentication.

```
device(config)# vlan 10
device(config-vlan-10# webauth
device(config-vlan-10-webauth)# accounting
```

acl-logging

Enables logging of entries in the syslog for packets that are denied by ACL filters.

Syntax

acl-logging

no acl-logging

Command Default

ACL logging is disabled by default.

Modes

Interface configuration mode

Usage Guidelines

Brocade devices support ACL logging of inbound packets that are sent to the CPU for processing (denied packets). ACL logging is not supported for outbound packets or any packets that are processed in hardware (permitted packets).

When you enable logging for ACL entries, statistics for packets that match the deny conditions of the ACL entries are logged. For example, if you configure a standard ACL entry to deny all packets from source address 10.157.22.26, statistics for packets that are explicitly denied by the ACL entry are logged in the Syslog buffer and in SNMP traps sent by the device.

You can enable ACL logging on physical and virtual interfaces.

ACL logging is not supported for dynamic ACLs with MAC authentication or 802.1X enabled.

NOTE
The **acl-logging** command is applicable to IPv4 devices only. For IPv6 devices, use the **logging-enable** command.

The **no** form of the command disables ACL logging.

Examples

The following example displays an ACL logging configuration on an IPv4 device.

```
device(config)# access-list 1 deny host 10.157.22.26 log
device(config)# access-list 1 deny 10.157.29.12 log
device(config)# access-list 1 deny host IPHost1 log
device(config)# access-list 1 permit any
device(config)# interface e 1/1/4
device(config-if-e1000-1/1/4)# acl-logging
device(config-if-e1000-1/1/4)# ip access-group 1 in
```

acl-mirror-port

Configures ACL-based inbound mirroring.

Syntax

acl-mirror-port ethernet *stackid/slot/port*

no acl-mirror-port ethernet *stackid/slot/port*

Parameters

ethernet *stackid/slot/port*

Specifies the mirror port to which the monitored port traffic is copied.

Modes

Interface configuration mode

Usage Guidelines

Use this command to set the destination port on which the traffic must be mirrored. The destination port must be the same for all ports in a port region. All traffic mirrored from any single port in a port region is mirrored to the same destination mirror port as traffic mirrored from any other port in the same port region. When a destination port is configured for any port within a port region, traffic from any ACL with a mirroring clause assigned to any port in that port region is mirrored to that destination port. This will occur even if a destination port is not explicitly configured for the port with the ACL configured.

To configure ACL-based mirroring for ACLs bound to virtual interfaces, use the **acl-mirror-port** command on a physical port that is a member of the same VLAN as the virtual interface. You can apply ACL-based mirroring on an entire VE, and enable mirroring in only one port region; traffic that is in the same VE but on a port in a different port region will not be mirrored. If a port is in both mirrored and non-mirrored VLANs, only traffic on the port from the mirrored VLAN is mirrored.

NOTE
If a destination mirror port is not configured for any ports within the port region where the port-mirroring ACL is configured, the ACL does not mirror the traffic but the ACL is applied to traffic on the port.

The **no** form of the command removes the ACL mirror port.

Examples

The following example shows the ACL mirroring traffic from port 1/1/1 is mirrored to port 1/1/3.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1)# acl-mirror-port ethernet 1/1/3
```

The following example shows that ports from a port region must be mirrored to the same destination mirror port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# acl-mirror-port ethernet 1/2/3
device(config)# interface ethernet 1/1/2
device(config-if-e10000-1/1/2)# acl-mirror-port ethernet 1/2/3
```

The following example shows ACL mirroring when the destination port within a port region is configured.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# ip access-group 101 in
device(config)# interface ethernet 1/1/3
device(config-if-e10000-1/1/3)# acl-mirror-port ethernet 1/4/3
```

The following example shows how to specify the destination mirror port for LAG ports.

```
device(config)# lag static
device(config-lag)# ports ethernet 1/1/1 to 1/14
device(config-lag)# deploy
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# acl-mirror-port ethernet 1/1/8
```

The following example shows how to configure ACL-based mirroring for ACLs bound to virtual interfaces.

```
device(config)# vlan 10
device(config-vlan-10)# tagged ethernet 1/4/1 to 1/4/2
device(config-vlan-10)# tagged ethernet 1/5/3
device(config-vlan-10)# router-interface ve 10
device(config-vlan-10)# exit
device(config)# interface ethernet 1/4/1
device(config-if-e10000-1/4/1)# acl-mirror-port ethernet 1/5/1
device(config-if-e10000-1/4/1)# exit
device(config)# interface ve 10
device(config-vif-10)# ip address 10.10.10.254/24
device(config-vif-10)# ip access-group 102 in
device(config)# access-list 102 permit ip any any mirror
```

The following example shows the ACL-based mirroring for ports in both mirrored and non-mirrored VLANs.

```
device(config)# vlan 10
device(config-vlan-10)# tagged ethernet 1/4/1 to 1/4/2
device(config-vlan-10)# tagged ethernet 1/5/3
device(config-vlan-10)# router-interface ve 10
device(config-vlan-10)# exit
device(config)# vlan 20
device(config-vlan-20)# tagged ethernet 1/4/1 to 1/4/2
device(config-vlan-20)# exit
device(config)# interface ethernet 1/4/1
device(config-if-e10000-1/4/1)# acl-mirror-port ethernet 1/5/1
device(config-if-e10000-1/4/1)# exit
device(config)# interface ve 10
device(config-vif-10)# ip address 10.10.10.254/24
device(config-vif-10)# ip access-group 102 in
device(config-vif-10)# exit
device(config)# access-list 102 permit ip any any mirror
```

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

add mac

Permanently authenticates certain hosts.

Syntax

add mac *mac-address* [**ethernet** *stavk/slot/port*] [**duration** *time*]

no add mac *mac-address* [**ethernet** *stack/slot/port*] [**duration** *time*]

Command Default

Permanent authentication is not enabled.

Parameters

mac-address
Specifies the MAC address of the host.

ethernet *stack/slot/port*
Specifies the Ethernet interface.

duration *time*
Specifies how long the MAC address remains authenticated. Valid values are from 0 through 128,000 seconds. The default is the time configured using the **reauth-time** command. If 0 is configured, then Web Authentication for the MAC address will not expire.

Modes

Web Authentication configuration mode

Usage Guidelines

Certain hosts, such as a DHCP server, gateway, or printers, may need to be permanently authenticated. Typically, these hosts are managed by the network administrator and are considered to be authorized hosts. Also, some of these hosts (such as printers) may not have a browser and will not be able to perform the Web Authentication.

NOTE
If a MAC address is statically configured, the MAC address will not be allowed to be dynamically configured on any port.

The **no** form of the command without any parameters removes all hosts and sets the duration a MAC address remains authenticated to its default.

Examples

The following example configures the host with MAC address 0000.00eb.2d14 to be permanently authenticated.

```
device(config)# vlan 10
device(config-vlan-10# webauth
device(config-vlan-10-webauth)# add mac 0000.00eb.2d14 duration 0
```

The following example specifies the MAC address to be added by the specified port that is a member of the VLAN.

```
device(config)# vlan 10
device(config-vlan-10# webauth
device(config-vlan-10-webauth)# add mac 0000.00eb.2d14 ethernet 1/1/1 duration 0
```

address-family

Enables the IPv4 or IPv6 address family configuration mode.

Syntax

address-family { **ipv4** | **ipv6** } [**max-route** *num*]

no address-family { **ipv4** | **ipv6** } [**max-route** *num*]

Command Default

Address family is not configured.

Parameters

ipv4

Specifies an IPv4 address family.

ipv6

Specifies an IPv6 address family.

max-route *num*

Configures the maximum number routes in a VRF. The valid range is from 128 through 15168. The default is 1024.

Modes

VRF 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 shows how to enable IPv4 address-family configuration mode:

```
device(config)# vrf red
device(config-vrf-red)# address-family ipv4
device(config-vrf-red-ipv4)#
```

address-family unicast (BGP)

Enables the IPv4 or IPv6 address family configuration mode to configure a variety of BGP4 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 the name of the VRF instance to associate with subsequent address-family configuration mode commands.

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

This example enables BGP IPv6 address family configuration mode.

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

This example creates a BGP4 unicast instance for VRF green.

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

History

Release version	Command history
8.0.30	Multi-VRF support was added for IPv6 BGP.

add-vlan

Adds individual VLANs or a range of VLANs.

Syntax

add-vlan *vlan-id* [**to** *vlan-id*]

Command Default

VLANs are added when creating a VLAN group.

Parameters

vlan-id

Specifies the VLAN ID to add.

to *vlan-id*

Specifies the range of VLANs to add.

Modes

VLAN group configuration mode

Usage Guidelines

Use the **vlan-group** command to add up to 256 VLANs. To add more than 256 VLANs, use the **add-vlan** command.

NOTE
The device memory must be configured to contain at least the number of VLANs you specify for the higher end of the range. For example, if you specify 2048 as the VLAN ID at the high end of the range, you first must increase the memory allocation for VLANs to 2048 or higher. Additionally, on Layer 3 switches, if you allocate additional memory for VLANs, you also need to allocate the same amount of memory for virtual routing interfaces before you configure the VLAN groups. This is true regardless of whether you use the virtual routing interface groups. The memory allocation is required because the VLAN groups and virtual routing interface groups have a one-to-one mapping.

Examples

The following example shows how to add VLANs.

```
device(config)# vlan-group 1 vlan 2 to 1000
device(config-vlan-group-1)# add-vlan 1001 to 1002
```

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 60 seconds by default. You can change the interval to be up to 3600 seconds 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)# tag ethernet 1/1/1 to 1/1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# backup
device(config-vlan-200-vrid-1)# activate
device(config-vlan-200-vrid-1)# advertise backup
```

age

Configures the device to age out secure MAC addresses after a specified amount of time.

Syntax

age *time* [**absolute**]

no age *time* [**absolute**]

Command Default

By default, learned MAC addresses stay secure indefinitely.

Parameters

time

Configures the age timer. Valid values range is from 0 through 1440 minutes. If you configure 0, the MAC addresses stay secure indefintely.

absolute

Configures all secure MAC addresses to age out immediately once the specified time expires.

Modes

Port security configuration mode

Port security interface configuration mode

Usage Guidelines

If the **absolute** keyword is not specified, secure MAC addresses are aged out only when the configured hardware MAC address age time expires.

NOTE
Even though you can set the age time to specific ports independent of the device-level setting, the age timer will take the greater of the two values. If you set the age timer to 3 minutes for the port, and 10 minutes for the device, the port MAC address aging occurs in 10 minutes (the device-level setting), which is greater than the port setting that you have configured.

On the Brocade ICX 7750, the port security age can only be set to the global hardware age. The absolute age and no aging of secure MACs are configured as static in hardware.

The **no** form of the command configures to never age out secure MAC addresses.

Examples

The following example sets the port security age timer to 10 minutes on all interfaces.

```
device(config)# port security
device(config-port-security)# age 10
```

The following example ages out secure MAC addresses immediately after one minute.

```
device(config)# port security
device(config-port-security)# age 1 absolute
```

The following example sets the port security age timer to 10 minutes on a specific interface.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)#port security
device(config-port-security-e1000-1/1/1)# age 10
```

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.

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.

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

Usage Guidelines

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

Examples

This example aggregates routes from a range of networks into a single network prefix and prevents the device from advertising more-specific routes.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# aggregate-address 10.11.12.0 summary-only
```

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

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# aggregate-address 2001:DB8:12D:1300::/64 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-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# aggregate-address 5.0.0.0/8
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

aggregated-vlan

Enables support for larger Ethernet frames.

Syntax

aggregated-vlan

no aggregated-vlan

Command Default

Support for larger Ethernet frames is not enabled.

Modes

Global configuration mode

Usage Guidelines

The command provides support for larger Ethernet frames up to 1536 bytes.

The **no** form of the command disables the support for larger Ethernet frames.

Examples

The following example shows how to provide support for larger Ethernet frames.

```
device(config)# aggregated-vlan
```

alias

An alias serves as a shorthand version of a longer CLI command.

Syntax

alias

alias *alias-name* **=** *cli-command*

no alias *alias-name*

unalias *alias-name*

Command Default

No aliases are defined.

Parameters

alias-name

Alias name. Must be a single word, without spaces.

=

Operator representing "equals."

cli-command

Command string for which the alias is created.

Modes

Privileged EXEC mode.

Global configuration mode.

Usage Guidelines

To remove an alias you can enter the **no alias** or the **unalias** command followed by the *alias-name*.

An alias saves typing in a longer command that you commonly use. For example, you can create an alias called *shoro* for the CLI command **show ip route**. Then when you enter *shoro* at the command prompt, the **show ip route** command is issued.

Entering the **alias** command with no parameters displays the currently configured aliases on the device.

Examples

The following example creates an alias called *shoro* for the CLI command **show ip route**, enter the **alias shoro = show ip route** command:

```
device(config)# alias shoro = show ip route
```

The following example uses the command **copy running-config** with the appropriate parameters to create an alias called *wrsbc*:

```
device(config)# alias wrsbc = copy running-config tftp 10.10.10.10 test.cfg
```

The following example removes the *wrsbc* alias from the configuration:

```
device(config)# no alias wrsbc
```

An alternate method of removing the alias is shown below:

```
device(config)# unalias wrsbc
```

To display the aliases currently configured on the Ruckus device, enter the following command at either the Privileged EXEC or global configuration modes of the CLI.

```
device# alias
          wrsbc      copy running-config tftp 10.10.10.10 test.cfg
          shoro       show ip route
```

all-client

Restricts all remote management access methods to a host.

Syntax

all-client { *ip-address* | **ipv6** *ipv6-address* }

no all-client { *ip-address* | **ipv6** *ipv6-address* }

Command Default

Remote management access is not restricted.

Parameters

ip-address

The IP address of the host to which you want to restrict the remote management access.

ipv6 *ipv6-address*

The IPv6 address of the host to which you want to restrict the remote management access.

Modes

Global configuration mode

Usage Guidelines

By default, a Brocade device does not control remote management access based on the IP address of the managing device. Using the **all-client** command, you can restrict remote management access to a single IP address for all of the following access methods:

- Telnet access
- SSH access
- Web management access
- SNMP access

You can specify only one IP address at a time. However, you can enter each command ten times to specify up to ten IP addresses.

The **no** form of the command removes the access restriction.

Examples

The following example shows how to restrict all remote management access methods to a host with IP address 10.157.22.69.

```
device(config)# all-client 10.157.22.69
```

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-router)# always-compare-med
```

always-propagate

Enables the device to reflect BGP routes even though they are not installed in the Routing Table Manager (RTM).

Syntax

always-propagate

no always-propagate

Command Default

This feature is disabled.

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

Usage Guidelines

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

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.

Examples

This example configures the device to reflect routes that are not installed in the RTM.

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

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

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

This example configures the device to reflect routes that are not installed in the RTM in a nondefault VRF instance.

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

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

anycast-rp

Configures PIM anycast rendezvous points (RPs) in IPv4 and IPv6 multicast domains.

Syntax

anycast-rp *rp-address anycast-rp-set-acl*

no anycast-rp *rp-address anycast-rp-set-acl*

Command Default

PIM anycast RPs are not configured.

Parameters

rp-address

Specifies a shared RP address used among multiple PIM routers.

anycast-rp-set-acl

Specifies a host-based simple access -control list (ACL) used to specify the address of the anycast RP set, including a local address.

Modes

PIM router configuration mode

Usage Guidelines

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

PIM anycast RP is a way to provide load balancing and fast convergence to PIM RPs in an IPv4 or IPv6 multicast domain. The RP address of the anycast RP is a shared address used among multiple PIM routers, known as PIM RP.

The PIM software supports up to eight PIM anycast RP routers. All deny statements in the my-anycast-rp-set-acl ACL are ignored.

Examples

This example shows how to configure a PIM anycast RP.

```
device(config)# router pim
device(config-pim-router)# rp-address 100.1.1.1
device(config-pim-router)# anycast-rp 100.1.1.1 my-anycast-rp-set-acl
```

This example shows how to configure PIM anycast RP 100.1.1.1.The example avoids using loopback 1 interface when configuring PIM Anycast RP because the loopback 1 address could be used as a router-id. A PIM first-hop router registers the source with the closest RP. The first RP that receives the register re-encapsulates the register to all other anycast RP peers.

```
Device(config)# interface loopback 2
Device(config-lbif-2)# ip address 100.1.1.1/24
Device(config-lbif-2)# ip pim-sparse
Device(config-lbif-2)# interface loopback 3
Device(config-lbif-3)# ip address 1.1.1.1/24
Device(config-lbif-3)# ip pim-sparse
Device(config-lbif-3)# router pim
Device(config-pim-router)# rp-address 100.1.1.1
Device(config-pim-router)# anycast-rp 100.1.1.1 my-anycast-rp-set
Device(config-pim-router)# ip access-list standard my-anycast-rp-set
Device(config-std-nacl)# permit host 1.1.1.1
Device(config-std-nacl)# permit host 2.2.2.2
Device(config-std-nacl)# permit host 3.3.3.
```

This example shows how to configure a PIM anycast RP for a VRF.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# rp-address 1001::1
Device(config-ipv6-pim-router-vrf-blue)# anycast-rp 1001::1 my-anycast-rp-set-acl
```

This example shows how to configure PIM anycast RP 1001:1 so that it avoids using loopback 1.

```
Device(config)# interface loopback 2
Device(config-lbif-2)# ipv6 address 1001::1/96
Device(config-lbif-2)# ipv6 pim-sparse
Device(config-lbif-2)# interface loopback 3
Device(config-lbif-3)# ipv6 address 1:1:1::1/96
Device(config-lbif-3)# ipv6 pim-sparse
Device(config-lbif-3)# ipv6 router pim
Device(config-ipv6-pim-router)# rp-address 1001::1
Device(config-ipv6-pim-router)# anycast-rp 1001::1 my-anycast-rp-set
Device(config-ipv6-pim-router)# ipv6 access-list my-anycast-rp-set
Device(config-std-nacl)# permit ipv6 host 1:1:1::1 any
Device(config-std-nacl)# permit ipv6 host 2:2:2::2 any
Device(config-std-nacl)# permit ipv6 host 3:3:3::3 any
```

arp-internal-priority

Configures the priority of ingress ARP packets.

Syntax

arp-internal-priority *priority-value*

Command Default

The default priority of ingress ARP packets is 4.

Parameters

priority-value

Specifies the priority value of the ingress ARP packets. It can take a value in the inclusive range of 0 to 7, where 7 is the highest priority.

Modes

Global configuration mode

Usage Guidelines

High traffic volume or non-ARP packets with a higher priority may cause ARP packets to be dropped, thus causing devices to become temporarily unreachable. You can use this command to increase the priority of ingress ARP packets. However, if the priority of ARP traffic is increased, a high volume of ARP traffic might cause drops in control traffic, possibly causing traffic loops in the network.

Stacking packets have a priority value of 7 and have higher precedence over ARP packets. If the ARP packets have priority value 7 in a stack system, they will be treated as priority value 6 packets when compared to stacking packets.

This command does not affect the priority of egress ARP packets.

You cannot change the priority of ingress ARP packets on the management port.

Examples

The following example sets the priority of ingress ARP packets to a value of 7.

```
Brocade(config)# arp-internal-priority 7
```

History

Release version	Command history
FastIron 08.0.01	This command was introduced.

as-path-ignore

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

Syntax

as-path-ignore

no as-path-ignore

Command Default

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-router)# as-path-ignore
```

atalk-proto

Configures the AppleTalk protocol-based VLAN.

Syntax

atalk-proto [**name** *string*]

no atalk-proto [**name** *string*]

Command Default

An AppleTalk protocol-based VLAN is not configured.

Parameters

name *string*

Specifies the name of the AppleTalk protocol you want to configure on a VLAN. The name can be up to 32 characters in length.

Modes

VLAN configuration mode

Usage Guidelines

The device sends AppleTalk broadcasts to all ports within the AppleTalk protocol-based VLAN.

The **no** form of the command disables the AppleTalk protocol-based VLAN.

Examples

The following example shows how to configure an AppleTalk protocol-based VLAN.

```
device(config)# vlan 10 by port
device(config-vlan-10)# untagged ethernet 1/1/1 to 1/1/6
added untagged port ethe 1/1/1 to 1/1/6 to port-vlan 30.
device(config-vlan-10)# atalk-proto name Atalk_Prot_VLAN
```

attempt-max-num

Configures the number of times a user can enter an invalid username and password; that is, the number of Web Authentication attempts during the specified cycle time.

Syntax

attempt-max-num *number*

no attempt-max-num *number*

Command Default

The default number of Web Authentication attempts allowed is five.

Parameters

number

Specifies the number of Web Authentication attempts. Valid values are from 0 through 64. If you configure 0, there is no limit on the number of attempts. The default is five attempts.

Modes

Web Authentication configuration mode

Usage Guidelines

You can set a limit on the number of times a user enters an invalid username and password during the specified cycle time. If the user exceeds the limit, the user is blocked for a duration of time, which is defined by the **block duration** command. Also, the Web browser will be redirected to the Exceeded Allowable Attempts web page.

The **no** form of the command sets the number of Web Authentication attempts to the default.

Examples

The following example limits the number of Web Authentication attempts to 10.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# attempt-max-num 10
```

auth-default-vlan

Specifies the auth-default VLAN globally.

Syntax

auth-default-vlan *vlan-id*

no auth-default-vlan *vlan-id*

Command Default

The auth-default VLAN is not specified.

Parameters

vlan-id

Specifies the VLAN ID of the auth-default VLAN.

Modes

Authentication configuration mode

Usage Guidelines

The auth-default VLAN must be configured to enable authentication.

A VLAN must be configured as auth-default VLAN to enable authentication. When any port is enabled for 802.1X authentication or MAC authentication, the client is moved to this VLAN by default.

The auth-default VLAN is also used in the following scenarios:

- When the RADIUS server does not return VLAN information upon authentication, the client is authenticated and remains in the auth-default VLAN.
- If RADIUS timeout happens during the first authentication attempt and the timeout action is configured as "Success", the client is authenticated in the auth-default VLAN. If the RADIUS server is not available during reauthentication of a previously authenticated client, the client is retained in the previously authenticated VLAN.

The **no** form of the command disables the auth-default VLAN.

Examples

The following example creates an auth-default VLAN with VLAN 2.

```
device(config)# authentication
device(config-authen)# auth-default-vlan 2
```

History

Release version	Command history
08.0.20	This command was introduced.

authenticate

Enables Network Time Protocol (NTP) strict authentication.

Syntax

authenticate

no authenticate

Command Default

Authentication is disabled.

Modes

NTP configuration mode

Usage Guidelines

If authentication is enabled, NTP packets not having a valid MAC address are dropped.

The **no** form of the command disables Network Time Protocol (NTP) strict authentication.

Examples

The following example shows how to enable authentication.

```
device(config)# ntp
device(config-ntp)# authenticate
```

authenticated-mac-age-time

Configures the time duration after which the user-associated MAC address is aged out and reauthentication is enforced.

Syntax

authenticated-mac-age-time *time*

no authenticated-mac-age-time *time*

Command Default

The default time is 3600 seconds.

Parameters

time

Specifies the time duration after which the user-associated MAC address is aged out and reauthentication is enforced. Valid values are 0 seconds to the reauthentication time configured using the **reauth-time** command. The default value is 3600 seconds.

Modes

Web Authentication configuration mode

Usage Guidelines

You can force Web Authenticated hosts to be reauthenticated if they have been inactive for a period of time. The inactive duration is calculated by adding the **mac-age-time** that has been configured for the device and the configured **authenticated-mac-age-time**. The **mac-age-time** command defines how long a port address remains active in the address table. If the authenticated host is inactive for the sum of these two values, the host is forced to be reauthenticated.

The **no** form of the command sets the time to the default of 3600 seconds.

Examples

The following example configures the time duration after which the user-associated MAC addressed is aged out and reauthentication is enforced.

```
device(config)# mac-age-time 600
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# reauth-time 303
device(config-vlan-10-webauth)# authenticated-mac-age-time 300
```

authentication

Enters the authentication mode.

Syntax

authentication

no authentication

Command Default

Authentication mode is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command will disable the authentication functionality.

Use this command to enter the authentication mode from global configuration mode. After entering authentication mode, you can configure additional authentication functionality that applies globally. Authentication functionality is also available for configuration at the interface configuration mode using different commands that apply only to the specified interface.

Examples

The following example enables authentication.

```
device(config)#authentication
device(config-authen)#
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication auth-default-vlan

Specifies the authentication default VLAN at the interface level.

Syntax

authentication auth-default-vlan *vlan-id*

no authentication auth-default-vlan *vlan-id*

Command Default

The auth-default VLAN is not specified.

Parameters

vlan-id

Specifies the VLAN ID of the auth-default VLAN.

Modes

Interface configuration mode

Usage Guidelines

The auth-default VLAN specified at the interface level overrides the auth-default VLAN configured using the **auth-default-vlan** command at the global level. The configured auth-default VLAN configured at the global level will still be applicable to other ports that don't have auth-default VLAN configured at the interface level.

The local auth-default VLAN must be configured to enable authentication.

A VLAN must be configured as auth-default VLAN to enable authentication. When any port is enabled for 802.1X authentication or MAC authentication, the client is moved to this VLAN by default.

The auth-default VLAN is also used in the following scenarios:

- When the RADIUS server does not return VLAN information upon authentication, the client is authenticated and remains in the auth-default VLAN.
- If RADIUS timeout happens during the first authentication attempt and the timeout action is configured as "Success", the client is authenticated in the auth-default VLAN. If the RADIUS server is not available during reauthentication of a previously authenticated client, the client is retained in the previously authenticated VLAN.

The **no** form of the command disables the auth-default VLAN.

Examples

The following example creates a default VLAN with VLAN 3.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication auth-default-vlan 3
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication auth-order

Specifies the sequence of authentication methods, 802.1X authentication and MAC authentication, on a specific interface.

Syntax

authentication auth-order {**dot1x mac-auth** | **mac-auth dot1x** }

no authentication auth-order {**dot1x mac-auth** | **mac-auth dot1x** }

Command Default

The authentication sequence is set to perform 802.1X authentication method followed by MAC authentication.

Parameters

dot1x mac-auth

Specifies 802.1X authentication followed by MAC authentication as the order of authentication methods on the interface.

mac-auth dot1x

Specifies MAC authentication followed by 802.1X authentication as the order of authentication methods on the interface.

Modes

Interface configuration mode

Usage Guidelines

If 802.1X authentication and MAC authentication methods are enabled on the same port, by default the authentication sequence is set to perform 802.1X authentication followed by MAC authentication.

Configuring the authentication order at the interface level overrides the configuration at the global level for that particular interface. The configured global authentication order will still be applicable to other ports that don't have a per port authentication order configured.

For authentication order 802.1X authentication followed by MAC authentication: When 802.1X authentication succeeds, the client is authenticated and the policies returned by the RADIUS server are applied. MAC authentication is not performed in this case. If 802.1X authentication fails, the failure action is carried out and MAC authentication is not attempted. On the other hand, if the client does not respond to dot1x messages, then MAC authentication is attempted. Upon successful MAC authentication, the client is authenticated and the policies returned by the RADIUS server are applied and on authentication failure, the configured failure action is applied.

For authentication order MAC authentication followed by 802.1X authentication: By default, 802.1X authentication is performed even if MAC authentication is successful. Upon successful 802.1X authentication, the client is authenticated and the policies returned by the RADIUS server are applied and on authentication failure, the configured failure action is applied. The default behavior can be changed by specifying the RADIUS attribute, to prevent the 802.1X authentication from being performed after successful MAC authentication. In this case, the client is authenticated and the policies returned by the RADIUS server are applied after successful MAC authentication. If MAC authentication method fails, 802.1X port security authentication is not attempted and the configured failure action is applied. However, if the **mac-authentication dot1x-override** command is configured, the clients that failed MAC authentication undergoes 802.1X authentication if the failure action is configured as restricted VLAN. If 802.1X authentication is successful, the policies returned by the RADIUS server are applied to the port.

The **no** form of the command disables the authentication order functionality.

Examples

The following example specifies 802.1X authentication followed by MAC authentication as the order of authentication methods on Ethernet interface 1/1/3.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/3
device(config-if-e1/1/3)# authentication auth-order dot1x mac-auth
```

The following example specifies MAC authentication followed by 802.1X authentication as the order of authentication methods on Ethernet interface 1/1/3.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/3
device(config-if-e1/1/3)# authentication auth-order mac-auth dot1x
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication auth-vlan-mode

Enables multiple-untagged mode on a specific Flexible authentication-enabled port and allows it to be member of multiple untagged VLANs.

Syntax

authentication auth-vlan-mode { **multiple-untagged** }

no authentication auth-vlan-mode { **multiple-untagged** }

Command Default

Flexible authentication-enabled port can be member of only one untagged VLAN.

Parameters

multiple-untagged

Allows the client to be assigned to multiple untagged VLANs on authentication.

Modes

Interface configuration mode

Usage Guidelines

Reload is not required to change the VLAN mode. However, existing sessions will be cleared if the command is applied to an individual interface.

The VLAN mode specified at the interface level overrides the VLAN mode configured using the **auth-vlan-mode** command at the global level. The configured VLAN mode configured at the global level will still be applicable to other ports that don't have the VLAN mode configured at the interface level.

Single untagged mode is only applicable to untagged VLANs returned by RADIUS.

The **no** form of the command returns the VLAN mode to single untagged. Port can be assigned to only one untagged VLAN on authentication.

Examples

The following example configures multiple untagged VLAN mode on interface 1/1/1.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
(config-if-e1000-1/1/1)# authentication auth-vlan-mode multiple-untagged
```

The following example clears all sessions on a Flexible authentication enabled interface and restores the single untagged VLAN mode.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
(config-if-e1000-1/1/1)# no authentication auth-vlan-mode multiple-untagged
```

History

Release version	Command history
08.0.30b	This command was introduced.

authentication disable-aging

Disables aging of MAC sessions at the interface level.

Syntax

authentication disable-aging { **permitted-mac-only** | **denied-mac-only** }

no authentication disable-aging { **permitted-mac-only** | **denied-mac-only** }

Command Default

Aging of MAC sessions is not disabled.

Parameters

permitted-mac-only

Prevents permitted (authenticated and restricted) sessions from being aged out and ages denied sessions.

denied-mac-only

Prevents denied sessions from being aged out, but ages out permitted sessions.

Modes

Interface configuration mode

Usage Guidelines

Use this command to disable the aging of MAC sessions. Use the **authentication disable-aging** command at the interface level and the **disable-aging** command in the authentication configuration mode. Entered at the interface level, this command overrides the command entered at the authentication global level. However, the global configuration to disable aging of MAC sessions will still be applicable to other ports that don't have configuration at the interface level.

The **no** form of the command does not disable aging.

Examples

The following example disables aging for permitted MAC addresses.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication disable-aging permitted-mac-only
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication dos-protection

Enables denial of service (DoS) authentication protection on the interface.

Syntax

authentication dos-protection { **enable** | **mac-limit** *mac-limit-value* }

no authentication dos-protection { **enable** | **mac-limit** *mac-limit-value* }

Command Default

Denial of service is disabled by default.

Parameters

enable

Specifies to enable DoS protection.

mac-limit

Specifies the maximum number MAC-authentication attempts allowed per second.

mac-limit-value

Specifies the rate limit for DoS protection. You can specify a rate from 1 - 65535 authentication attempts per second. The default is a rate of 512 authentication attempts per second.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables DoS protection.

To limit the susceptibility of the Brocade device to DoS attacks, you can configure the device to use multiple RADIUS servers, which can share the load when there are a large number of MAC addresses that need to be authenticated. The Brocade device can run a maximum of 10 RADIUS clients per server and will attempt to authenticate with a new RADIUS server if current one times out.

In addition, you can configure the Brocade device to limit the rate of authentication attempts sent to the RADIUS server. When MAC authentication is enabled, the number of RADIUS authentication attempts made per second is tracked. When you also enable the DoS protection feature, if the number of RADIUS authentication attempts for MAC addresses learned on an interface per second exceeds a configurable rate (by default 512 authentication attempts per second), the device considers this a possible DoS attack and disables the port. You must then manually re-enable the port.

Examples

The example specifies the DoS protection count as 256.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/3/1
device(config-if-e1000-1/3/1)# authentication dos-protection mac-limit 256
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication fail-action

Specifies the authentication failure action to move the client port to the restricted VLAN after authentication failure for both MAC authentication and 802.1X authentication on an interface.

Syntax

authentication fail-action restricted-vlan *vlan-id*

no authentication fail-action restricted-vlan

Command Default

The default action is to block the MAC address of the client.

Parameters

restricted-vlan

Specifies the failure action to move the client port to the restricted VLAN after authentication failure.

vlan-id

Specifies the ID of the VLAN to be configured as restricted VLAN.

Modes

Interface configuration mode

Usage Guidelines

If the authentication failure action is not configured, the client's MAC address is blocked in the hardware (default action) when the authentication fails.

The restricted VLAN specified at the interface level overrides the restricted VLAN configured using the **restricted-vlan** command at the global level. The configured restricted VLAN configured at the global level will still be applicable to other ports that don't have restricted VLAN configured at the interface level.

The client ports that were placed in the RADIUS-specified VLAN upon successful authentication are not placed in the restricted VLAN if the subsequent authentication fails. Instead, the non-authenticated client is blocked.

The **no** form of the command disables the authentication failure action.

Examples

The following example specifies authentication failure action to move the client port to the restricted VLAN (VLAN 4 is configured as restricted VLAN) after authentication failure.

```
device(config)# authentication
device(config-authen)# restricted-vlan 4
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication fail-action restricted-vlan 5
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication filter-strict-security

Enables or disables strict filter security for 802.1X and MAC-authentication enabled interfaces.

Syntax

authentication filter-strict-security

no authentication filter-strict-security

Command Default

Strict filter security is enabled.

Modes

Interface configuration mode

Usage Guidelines

When strict security mode is enabled, authentication for a port fails if the Filter-Id attribute contains invalid information, or if insufficient system resources are available to implement the IP ACLs.

When strict security mode is enabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, IP ACL configured on the device), then the client will not be authorized, regardless of any other information in the message (for example, if the Tunnel-Private-Group-ID attribute specifies a VLAN on which to assign the port).
- If the device does not have the system resources available to dynamically apply a filter to a port, then the client will not be authenticated.

When strict filter security is disabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, a MAC address filter or IP ACL configured on the device), then the client remains authorized and no filter is dynamically applied to it.
- By default, strict security mode is enabled for all MAC authentication and 802.1X-enabled interfaces, but you can manually disable or enable it using the **filter-strict-security** command from the authentication configuration mode or using the **authentication filter-strict-security** command from the interface configuration mode.

The **no** form of the command disables strict filter security.

Examples

The following example enables strict filter security.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication filter-strict-security
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.30mb	This command was modified.

authentication-key

Defines an authentication key for Network Time Protocol (NTP).

Syntax

authentication-key key-id *key-id* { **md5** | **sha1** } *key-string*

no authentication-key key-id *key-id* [**md5** | **sha1**] *key-string*

Command Default

Authentication keys are not configured.

Parameters

key-id

Specifies a valid key id. The value can range from 1 to 65535.

md5

The message authentication support that is provided using the Message Digest 5 Algorithm.

sha1

Specifies that the SHA1 keyed hash algorithm is used for NTP authentication.

key-string

The value of the MD5 or SHA1 key. The maximum length of the key string may be defined up to 16 characters. Up to 32 keys may be defined.

Modes

NTP configuration mode

Usage Guidelines

If JITC is enabled, only the **sha1** option is available.

If the NTP server/peer is configured without authentication keys, the NTP request is not sent to the configured server/peer.

The same set or subset of key id and key string should be installed on all NTP devices.

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

Examples

The following example shows how to configure an authentication key.

```
device(config)# ntp
device(config-ntp)# authentication-key key-id 1 md5 moof
```

authentication max-sessions

Specifies the maximum number of MAC sessions that can be authenticated per port for MAC authentication and 802.1X authentication.

Syntax

authentication max-sessions *count*

no authentication max-sessions *count*

Command Default

The default number of MAC sessions that can be authenticated on a single interface is 2.

Parameters

count

Specifies the maximum number of authenticated MAC sessions per port.

Modes

Interface configuration mode

Usage Guidelines

The maximum number of authenticated mac-sessions on an interface depends on the Brocade device and dynamic ACL assignments.

If RADIUS assigns dynamic ACL to at least one client on the interface, the maximum number of MAC sessions that can be authenticated is limited to 32 in all Brocade devices.

If dynamic ACL is not assigned to any of the clients on the interface, the maximum number of MAC addresses that can be authenticated varies depending on the Brocade device as specified in Table 5.

System reload is not required for the changes to take effect. However, existing sessions on the interface are cleared for the changes to take effect.

TABLE 5 Maximum number of authenticated MAC sessions per port on various platforms

Supported platforms	Maximum number of MAC sessions per port when none of the Clients has dynamic ACL	Maximum number of MAC sessions per port when at least one User has Dynamic ACL
ICX 6610	256	32
FCX	256	32
ICX 7750	1024	32
ICX 7450	1024	32
ICX 7250	1024	32
ICX 6450	256	32
ICX 6430	256	32

The system limit for authenticated MAC sessions also varies and depends on the Brocade device and dynamic ACL assignments.

TABLE 6 Maximum number of authenticated MAC sessions per system (standalone or stack) on various platforms

Supported platforms	Maximum number of MAC sessions per system when none of the clients has dynamic ACL	Maximum number of MAC sessions per system when at least one client has dynamic ACL
ICX 6610	1536	512
FCX	1536	512
ICX 7750	1536	512
ICX 7450	1536	512
ICX 7250	1536	512
ICX 6450	1536	512
ICX 6430	400	150

The **no** form of the command reinstates the maximum authenticated MAC sessions allowed per port to the default value of 2.

Examples

The example specifies the maximum number of authenticated MAC sessions.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication max-sessions 30
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.30b	The command was made available on Brocade ICX 7250, Brocade ICX 7450, and Brocade ICX 7750. The maximum number of authenticated MAC sessions per port was increased from 32 to 256 and 1024, depending on the platforms.

authentication reauth-timeout

Sets the time to wait before reauthenticating a client after a timeout-action (success, failure, or critical-vlan) is applied. This command is applicable for MAC authentication and 802.1X authentication.

Syntax

authentication reauth-timeout *seconds*

no authentication reauth-timeout *seconds*

Command Default

The default re-authentication timeout is 60 seconds.

Parameters

seconds

Sets the re-authentication timeout, in seconds. The range is from 60 to 4294967295.

Modes

Interface configuration mode

Usage Guidelines

The **no** form disables re-authentication timeout.

This command sets the re-authentication timeout at the interface level after the timeout action is specified as success, restricted VLAN or critical VLAN.

Examples

The example shows specifying a re-authentication timeout of 100 seconds.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/2
device(config-if-e1000-1/1/2)# authentication reauth-timeout 100
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication source-guard-protection enable

Enables Source Guard Protection along with authentication on a specified interface.

Syntax

authentication source-guard-protection enable

no authentication source-guard-protection enable

Command Default

Source Guard Protection is not enabled.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables source guard protection.

When a new MAC session begins on a port that has Source Guard Protection enabled, the session either applies a dynamically created Source Guard ACL entry or it uses the dynamic IP ACL assigned by the RADIUS server. If a dynamic IP ACL is not assigned, the session uses the Source Guard ACL entry. The Source Guard ACL entry is **permit ip** *secure-ip* **any**, where *secure-ip* is obtained from the ARP Inspection table or from the DHCP Secure table. The DHCP Secure table is comprised of DHCP Snooping and Static ARP Inspection entries. The Source Guard ACL permit entry is added to the hardware table after all of the following events occur:

- The MAC address is authenticated
- The IP address is learned
- The MAC-to-IP mapping is checked against the Static ARP Inspection table or the DHCP Secure table

The Source Guard ACL entry is not written to the running configuration file. However, you can view the configuration using the **show mac-authentication configuration** command at the global level or for a specific interface.

> **NOTE**
> The secure MAC-to-IP mapping is assigned at the time of authentication and remains in effect as long as the MAC session is active. The existing MAC session doesn't get affected if the DHCP Secure table is updated after the session is authenticated and while the session is still active.

The Source Guard ACL permit entry is removed when the MAC session expires or is cleared.

Examples

The following example enables source guard protection on an interface.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication source-guard-protection enable
```

History

Release version	Command history
08.0.20	This command was introduced.

authentication timeout-action

Configures the authentication timeout actions to specify the action for the RADIUS server if an authentication timeout occurs.

Syntax

authentication timeout-action { **success** | **failure** | **critical-vlan** }

no authentication timeout-action { **success** | **failure** | **critical-vlan** *vlan-id*}

Command Default

The default authentication timeout action is failure.

Parameters

success

Considers the client as authenticated after RADIUS timeout. After the timeout action is enabled as success, use the **no** form of the command to set the RADIUS timeout behavior to retry.

failure

Specifies the RADIUS timeout action to carry out the configured failure action. If the failure action is not configured, the client's MAC address is blocked in the hardware. Once the failure timeout action is enabled, use the **no** form of the command to reset the RADIUS timeout behavior to retry.

critical-vlan

Specifies to move the client to the specified critical VLAN after authentication timeout. This command applies only to data traffic.

vlan-id

Specifies the ID of the VLAN to be configured as critical VLAN.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command will disable this functionality.

If the timeout is configured as success, client will be authenticated in the auth-default VLAN.

If the authentication failure action is configured as restricted VLAN using the **authentication fail-action** command, the client is placed in the restricted VLAN. A restricted VLAN must be configured using the **restricted-vlan** command at the global level or using the **authentication fail-action restricted-vlan** command at the interface level.

The critical VLAN specified at the interface level overrides the critical VLAN configured using the **critical-vlan** command at the global level. The configured critical VLAN configured at the global level will still be applicable to other ports that don't have critical VLAN configured at the interface level.

Examples

The following example sets the **authentication timeout-action** command to success.

```
device(config)# authentication
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# authentication timeout-action success
```

History

Release version	Command history
08.0.20	This command was introduced.

auth-fail-action (802.1X authentication)

Configures all ports on the device to place the client port in a restricted VLAN when dot1x port authentication fails.

Syntax

auth-fail-action restricted-vlan

no auth-fail-action restricted-vlan

Command Default

Client traffic is dropped in the hardware.

Parameters

restricted-vlan

Specifies to place the client port in a restricted VLAN when the authentication fails.

Modes

dot1x configuration mode

Usage Guidelines

If the restricted VLAN is not specified using the **auth-fail-vlanid** command, the client port is placed in the default VLAN upon authentication failure.

The client ports that were placed in the RADIUS-specified VLAN upon successful authentication are not placed in the restricted VLAN if the subsequent authentication fails. Instead, the non-authenticated client is blocked.

The **no** form of this command disables the authentication failure action of placing the client port in a restricted VLAN.

Examples

The following example configures all ports on the device to place the client port in a restricted VLAN when the authentication fails.

```
device(config)# dot1x-enable
device(config-dot1x)# auth-fail-action restricted-vlan
```

History

Release version	Command history
08.0.20	This command was replaced on Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750 by the **auth-fail-action (Flexible authentication)** command.

auth-fail-action (Flexible authentication)

Specifies to move the client port to the restricted VLAN after authentication failure for both MAC authentication and 802.1X authentication globally.

Syntax

auth-fail-action restricted-vlan

no auth-fail-action restricted-vlan

Command Default

The MAC address of the client is blocked in the hardware.

Parameters

restricted-vlan

Specifies the failure action to move the client port to the restricted VLAN after authentication failure.

Modes

Authentication configuration mode

Usage Guidelines

A restricted VLAN must be configured using the **restricted-vlan** command before setting the fail action as restricted-vlan to move the client port to the restricted VLAN.

If the authentication failure action is not configured, the client's MAC address is blocked in the hardware (default action) when the authentication fails.

In single untagged mode, the client ports that were placed in the RADIUS-specified VLAN upon successful authentication are not placed in the restricted VLAN if the subsequent authentication fails. Instead, the non-authenticated client is blocked.

The **no** form of the command disables the authentication failure action.

Examples

The following example specifies authentication failure action to move the client port to the restricted VLAN (VLAN 4 is configured as restricted VLAN) after authentication failure.

```
device(config)# authentication
device(config-authen)# restricted-vlan 4
device(config-authen)# auth-fail-action restricted-vlan
```

History

Release version	Command history
08.0.20	This command was introduced.

auth-fail-force-restrict

Moves the native VLAN mac-sessions to a restricted VLAN on authentication failure.

Syntax

auth-fail-force-restrict

no auth-fail-force-restrict

Modes

dot1x configuration mode

Usage Guidelines

Use this command when you configure MAC authentication and 802.1X authentication configuration with dynamic VLAN assignment from a RADIUS server on the same port.

This command allows you to override the dual-mode port native untagged VLAN with restricted VLAN in case 802.1x authentication fails and there is no RADIUS assigned VLAN.

The **no** form of the command disables the configuration to move the native VLAN mac-sessions to a restricted VLAN on authentication failure.

Examples

The following example moves the native VLAN mac-sessions to a restricted VLAN on authentication failure.

```
device(config)# dot1x-enable
device(config-dot1x)# auth-fail-force-restrict
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

auth-fail-max-attempts

Configures the number of authentication attempts the device makes before taking the authentication failure action.

Syntax

auth-fail-max-attempts *number*

no auth-fail-max-attempts *number*

Command Default

The device makes three attempts to authenticate a client before taking the authentication failure action.

Parameters

number

Specifies the number of attempts to authenticate a client before taking the authentication failure action. The number of authentication attempts can be from 1 through 10.

Modes

dot1x configuration mode

Usage Guidelines

If authentication for the client is unsuccessful more than the number of times specified by the *number* variable in the **auth-fail-max-attempts** command, an authentication failure action is taken. The authentication failure action can be either to drop traffic from the client, or to place the port in a restricted VLAN:

- If the authentication failure action is to drop traffic from the client, then the client dot1x MAC session is set to "access-denied", causing traffic from the client to be dropped in hardware.
- If the authentication failure action is to place the port in a restricted VLAN, and the client dot1x MAC session is set to "access-restricted", then the port is moved to the specified restricted VLAN, and traffic from the client is forwarded normally.

The **no** form of the command reinstates the number of authentication attempts to the default value of 3.

Examples

The following example limits the number of authentication attempts to 2.

```
device(config)# dot1x-enable
device(config-dot1x)# auth-fail-max-attempts 2
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

auth-fail-vlanid

Configures a specific VLAN as the restricted VLAN for all ports on the device to place the client port when the authentication fails.

Syntax

auth-fail-vlanid *vlan-id*

no auth-fail-vlanid *vlan-id*

Command Default

The restricted VLAN is not configured.

Parameters

vlan-id

Specifies the identification number of the VLAN to be used as the restricted VLAN.

Modes

dot1x configuration mode

Usage Guidelines

When an authentication fails, the port can be moved to a configured restricted VLAN instead of failing the client completely. The port is moved to the configured restricted VLAN only if the authentication failure action is set to place the port in a restricted VLAN using the **auth-fail-action** command.

The **no** form of the command removes the restricted VLAN configuration on the VLAN.

Examples

The following example specifies VLAN 300 as the restricted VLAN for all ports on the device.

```
device(config)# dot1x-enable
device(config-dot1x)# auth-fail-vlanid 300
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

auth-mode captive-portal

Authenticates the users in a VLAN through external Web Authentication (Captive Portal user authentication mode).

Syntax

auth-mode captive-portal

no auth-mode captive-portal

Command Default

External Web Authentication mode is not enabled by default.

Modes

Web Authentication configuration mode

Usage Guidelines

External Web Authentication uses RADIUS as the authentication method.

The **no** form of the command removes the external Web Authentication mode as the configured authentication mode.

Examples

The following example configures the authentication mode as external Web Authentication to authenticate the users in a VLAN.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode captive-portal
```

History

Release version	Command history
8.0.40	This command was introduced.
8.0.30j	This command was added to FastIron 8.0.30j

auth-mode none

Enables automatic Web Authentication.

Syntax

auth-mode none

no auth-mode none

Command Default

By default, if Web Authentication is enabled, hosts need to login and enter authentication credentials to gain access to the network.

Modes

Web Authentication configuration mode

Usage Guidelines

If a reauthentication period is configured, the host will be asked to re-enter authentication credentials once the reauthentication period ends.

You can configure Web Authentication to authenticate a host when the user clicks the **Login** button. When a host enters a valid URL address, Web Authentication checks the list of blocked MAC addresses. If the host's MAC address is not on the list and the number of allowable hosts has not been reached, after clicking the **Login** button, the host is automatically authenticated for the duration of the configured reauthentication period, if one is configured. Once the reauthentication period ends, the host is logged out and must enter the URL address again. If automatic authentication is enabled and a host address is not in the blocked MAC address list, Web Authentication authenticates the host and displays the Login page without user credentials, and then provides a hyperlink to the requested URL site.

> **NOTE**
> Automatic authentication is not the same as permanent authentication. You must still specify devices that are to be permanently authenticated even if automatic authentication is enabled.

Use the **show webauth vlan** command in VLAN configuration mode to determine if automatic authentication is enabled.

The **no** form of the command removes the automatic Web Authentication configuration.

Examples

The following example enables automatic Web Authentication.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode none
```

auth-mode passcode

Enables Web Authentication to use dynamically created passcodes to authenticate users in the VLAN.

Syntax

auth-mode passcode [**flush-expired** | **generate** | **grace-period** *time* | **length** *passcode-length* | **log** { **snmp-trap** | **syslog** } | **refresh-type** { **duration** *time* | **time** [*time-string* | **delete-all**] } | **resend-log** | **static**]

no auth-mode passcode [**flush-expired** | **generate** | **grace-period** *time* | **length** *passcode-length* | **log** { **snmp-trap** | **syslog** } | **refresh-type** { **duration** *time* | **time** [*time-string* | **delete-all**] } | **resend-log** | **static**]

Command Default

Passcode authentication is not enabled.

Parameters

flush-expired
Deletes old passcodes that have expired but are still valid because they are in the grace period.

generate
Refreshes the passcode instead of waiting for the system to automatically generate one.

grace-period *time*
Configures a grace period for an expired passcode.

length *passcode-length*
Configures the passcode length. Valid values are from 4 through 16 digits. The default is 4 digits.

log
Enables the generation of syslog messages and SNMP trap messages every time a new passcode is generated and passcode authentication is attempted. By default, the syslog and SNMP trap messages are enabled.

snmp-trap
Generates SNMP trap messages every time a new passcode is generated and passcode authentication is attempted.

syslog
Generates syslog messages every time a new passcode is generated and passcode authentication is attempted.

refresh-type
Configures the passcode refresh type as one of the following:

duration *time*
Configures the duration of time after which passcodes are refreshed. By default, dynamically created passcodes are refreshed every 1440 minutes (24 hours).

time *time-string*
Configures the time of the day when the passcode should be refreshed. When initially enabled, the time of day method will cause passcodes to be refreshed at 00:00 (12:00 midnight). You can add up to 24 refresh periods in a 24-hour period.

delete-all
Deletes all of the configured passcode refresh times and reverts back to the default time of 00:00 (12:00 midnight).

resend-log

Retransmits the current passcode to a syslog message or SNMP trap if passcode logging is enabled.

static

Creates a static passcode.

Modes

Web Authentication configuration mode

Usage Guidelines

You can delete old passcodes that have expired but are still valid because they are in the grace period using the **auth-mode passcode flush-expired** command. This is useful in situations where the old passcodes have been compromised but are still valid because of the grace period. This command does not affect current valid passcodes or passcodes that newly expire.

When manually refreshed using the **auth-mode passcode generate** command, the old passcode will no longer work, even if a grace period is configured. Also, if the passcode refresh method duration of time is used, the duration counter is reset when the passcode is manually refreshed. The passcode refresh method time of day is not affected when the passcode is manually refreshed.

If the grace period is reconfigured using the **auth-mode passcode grace-period** command while a passcode is already in the grace period, the passcode is not affected by the configuration change. The new grace period will apply only to passcodes that expire after the new grace period is set.

If you change the passcode refresh value using the **auth-mode passcode refresh-type**, the configuration is immediately applied to the current passcode. If both the duration of time and time of day passcode refresh values are configured, they are saved to the configuration file. You can switch back and forth between the passcode refresh methods, but only one method can be enabled at a time.

Passcodes are not stateful, meaning a software reset or reload will cause the system to erase the passcode. When the device comes back up, a new passcode will be generated.

When the **auth-mode passcode resend-log** command is configured, the switch retransmits the current passcode only. Passcodes that are in the grace period are not sent.

Static passcodes can be used for troubleshooting purposes, or for networks that want to use passcode authentication, but do not have the ability to support automatically generated passcodes (for example, the network does not fully support the use of SNMP traps or syslog messages with passcodes). Manually created passcodes are used in conjunction with dynamic passcodes . You can configure up to four static passcodes that never expire. Unlike dynamically created passcodes, static passcodes are saved to flash memory. By default, there are no static passcodes configured on the switch. Static passcodes do not have to be the same length as passcodes that are automatically generated.

Use the **show webauth vlan** *vlan-id* **passcode** command to view the current passcodes.

The **no** form of the command removes or disables the configured settings.

Examples

The following example flushes out all expired passcodes that are currently in the grace period.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode flush-expired
```

The following example refreshes the passcode immediately.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode generate
```

The following example configures the grace period for an expired passcode.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode grace-period 5
```

The following example increases the passcode length to 10 digits.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode length 10
```

The following example shows how to re-enable syslog messages for passcodes after they have been disabled.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode log syslog
```

The following example changes the duration of time after which passcodes are refreshed to 4320 minutes (72 hours).

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode refresh-type duration 4320
```

The following example configures the switch to refresh passcodes at a certain time of day.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode refresh-type time 14:30
```

The following example deletes all of the configured passcode refresh times and reverts back to the default time of 00:00 (12:00 midnight).

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode refresh-type time delete-all
```

The following example retransmits the current passcode to a syslog message or SNMP trap if passcode logging is enabled.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode resend-log
```

The following example creates static passcodes.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode passcode static 3267345
```

auth-mode username-password

Enables the username and password Web Authentication mode.

Syntax

auth-mode username-password [**auth-methods** {**radius** [**local**] | **local** [**radius**] } | **local-user-database** *database-name*]

no auth-mode username-password [**auth-methods** {**radius** [**local**] | **local** [**radius**] } | **local-user-database** *database-name*]

Command Default

Username password authentication is not enabled.

Parameters

auth-methods
Configures the authentication method.

radius
Uses the RADIUS server to authenticate.

local
Uses the local user database to authenticate.

local-user-database *database-name*
Uses the usernames and passwords in the specified database to authenticate.

Modes

Web Authentication configuration mode

Usage Guidelines

You can optionally specify a failover sequence for RADIUS and local user database authentication methods. For example, you can configure Web Authentication to first use a local user database to authenticate users in a VLAN. If the local user database is not available, it will use a RADIUS server. You can specify the **local** and **radius** options one after the other in the required sequence to configure the failover sequence.

The **no** form of the command removes the username password authentication.

Examples

The following example uses a local user database to authenticate users in a VLAN.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode username-password auth-methods local
```

The following example uses the usernames and passwords in the specified database to authenticate.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode username-password local-user-database
```

The following example configures a failover sequence for RADIUS and local user database authentication methods. In this example, Web Authentication first uses a local user database to authenticate users in a VLAN. If the local user database is not available, it will use a RADIUS server.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# auth-mode username-password auth-methods local radius
```

auth-order

Specifies the sequence of authentication methods, 802.1X authentication and MAC authentication at the global level.

Syntax

auth-order {**dot1x mac-auth** | **mac-auth dot1x** }

no auth-order {**dot1x mac-auth** | **mac-auth dot1x** }

Command Default

The authentication sequence is set to perform 802.1X authentication method followed by MAC authentication.

Parameters

dot1x mac-auth

Specifies 802.1X authentication followed by MAC authentication as the order of authentication methods on the interface.

mac-auth dot1x

Specifies MAC authentication followed by 802.1X authentication as the order of authentication methods on the interface.

Modes

Authentication configuration mode

Usage Guidelines

If 802.1X authentication and MAC authentication methods are enabled on the same port, by default the authentication sequence is set to perform 802.1X authentication followed by MAC authentication.

For authentication order 802.1X authentication followed by MAC authentication: When 802.1X authentication succeeds, the client is authenticated and the policies returned by the RADIUS server are applied. MAC authentication is not performed in this case. If 802.1X authentication fails, the failure action is carried out and MAC authentication is not attempted. On the other hand, if the client does not respond to 802.1X messages, then MAC authentication is attempted. Upon successful MAC authentication, the client is authenticated and the policies returned by the RADIUS server are applied and on authentication failure, the configured failure action is applied.

For authentication order MAC authentication followed by 802.1X authentication: By default, 802.1X authentication is performed even if MAC authentication is successful. Upon successful 802.1X authentication, the client is authenticated and the policies returned by the RADIUS server are applied and on authentication failure, the configured failure action is applied. The default behavior can be changed by specifying the RADIUS attribute, to prevent the 802.1X authentication from being performed after successful MAC authentication. In this case, the client is authenticated and the policies returned by the RADIUS server are applied after successful MAC authentication. If MAC authentication method fails, 802.1X port security authentication is not attempted and the configured failure action is applied. However, if the **mac-authentication dot1x-override** command is configured, the clients that failed MAC authentication undergoes 802.1X authentication if the failure action is configured as restricted VLAN. If 802.1X authentication is successful, the policies returned by the RADIUS server are applied to the port.

The **no** form of the command disables the authentication order functionality.

Examples

The following example specifies 802.1X authentication followed by MAC authentication as the order of authentication methods at the global level.

```
device(config)# authentication
device(config-authen)# auth-order dot1x mac-auth
```

The following example specifies MAC authentication followed by 802.1X authentication as the order of authentication methods at the global level.

```
device(config)# authentication
device(config-authen)# auth-order mac-auth dot1x
```

History

Release version	Command history
08.0.20	This command was introduced.

auth-vlan-mode

Enables the Flexible authentication-enabled ports to be member of multiple untagged VLANs.

Syntax

auth-vlan-mode { **multiple-untagged** }

no auth-vlan-mode { **multiple-untagged** }

Command Default

Flexible authentication-enabled port can be member of only one untagged VLAN.

Parameters

multiple-untagged

Allows the client to be assigned to multiple untagged VLANs on authentication.

Modes

Authentication configuration mode

Usage Guidelines

Reload is not required to change the VLAN mode. If the command is applied globally, all sessions will be cleared on all interfaces that have Flexible authentication enabled. However, existing sessions will be cleared if the command is applied on an individual interface using the **authentication auth-vlan-mode** command from the interface configuration mode.

Single untagged mode is only applicable to untagged VLANs returned by RADIUS.

The **no** form of the command returns the VLAN mode to single untagged. Port can be assigned to only one untagged VLAN on authentication.

Examples

The following example configures multiple untagged VLAN at the global level.

```
device# configure terminal
device(config)# authentication
device(config-authen)# auth-vlan-mode multiple-untagged
```

The following example clears all sessions on interfaces with Flexible authentication enabled and restores the single untagged VLAN mode default on all new sessions established on those interfaces.

```
device# configure terminal
device(config)# authentication
device(config-authen)# no auth-vlan-mode multiple-untagged
```

History

Release version	Command history
08.0.30b	This command was introduced.

auto-cost reference-bandwidth (OSPF)

Configures reference bandwidth.

Syntax

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

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

ref-bw

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

use-active-ports

When set, 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

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.

Enter **no auto-cost reference-bandwidth** to disable bandwidth configuration.

Examples

This example configures a reference bandwidth of 500.

```
device# configure
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 *ref-bw*

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

ref-bw

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

Modes

OSPFv3 router configuration mode

Usage Guidelines

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

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

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

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

NOTE
If you specify the cost for an individual interface (by using the **ipv6 ospf cost** command), the cost you specify overrides the cost calculated by the software.

Enter **no auto-cost reference-bandwidth** to disable bandwidth configuration.

Examples

This 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.

autosave

Automatically saves learned secure MAC addresses to the startup configuration at specified intervals.

Syntax

autosave *time*

no autosave *time*

Command Default

By default, secure MAC addresses are not autosaved to the startup-config file.

Parameters

time

The interval between two autosaves, in minutes. The valid range is from 15 to1440 minutes.

Modes

Port security configuration mode

Port security interface configuration mode

Usage Guidelines

The autosave feature saves learned MAC addresses by copying the running configuration to the startup configuration.

If you change the autosave interval, the next save occurs according to the old interval, and then the new interval takes effect. To change the interval immediately, disable autosave by entering the **no autosave** command, and then configure the new autosave interval using the **autosave** command.

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

Examples

The following example saves learned secure MAC addresses every 20 minutes automatically.

```
device(config)# port security
device(config-port-security)# autosave 20
```

The following example saves learned secure MAC addresses every 20 minutes automatically on an interface.

```
device(config)# port security
device(config-port-security)# interface ethernet 1/1/1
device(config-port-security-e1000-1/1/1)# autosave 20
```

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 5.

Parameters

priority *priority-number*
: Configures the backup priority for the VSRP VRID. The range is from 6 through 255. The default value is 100.

track-priority *track-number*
: Configures the track priority for the VSRP VRID. The range is from 1 through 254. The default value is 5.

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 1/1/1 to 1/1/8
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 1/1/1 to 1/1/8
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-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 60 seconds by default.

Parameters

number

Specifies the time interval for the backup to send the Hello messages. The time range is from 60 through 3600 seconds.

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 1/1/1 to 1/1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# backup
device(config-vlan-200-vrid-1)# activate
device(config-vlan-200-vrid-1)# backup-hello-interval 180
```

bandwidth (interface)

Sets and communicates bandwidth value for an interface to higher-level protocols such as OSPFv2 and OSPFv3, so this setting can be used to influence the routing cost for routes learnt on these interfaces.

Syntax

bandwidth { *kilobits* }

no bandwidth { *kilobits* }

Command Default

For physical ports, the port speed is the default bandwidth. For VE interfaces and Link aggregation (LAG) groups, the sum of port speeds of individual physical ports is the default bandwidth.

Parameters

kilobits

Intended bandwidth, in kilobits per second. There is no default value for this parameter. The range is from 1 to 1000000000 kbps (100 Gbps).

Modes

Interface configuration mode.

Usage Guidelines

Use the **no bandwidth** command to remove the bandwidth value.

This command is supported on all Brocade FastIron platforms.

You cannot adjust the actual bandwidth of an interface with this command. When you configure the interface bandwidth for virtual Ethernet that is associated with multiple physical interfaces, OSPF does not adjust its metric cost if one of those associated interfaces is down, and does not generate network and router link state advertisement.

This command is

Examples

This example sets the bandwidth to 2000 kbps on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1) bandwidth 2000
```

This example sets the bandwidth to 2000 kbps on a specific virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# interface ve 10
device(config-vif-10) bandwidth 2000
```

This example sets the bandwidth to 2000 kbps on a specific tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 2
device(config-tnif-2) bandwidth 2000
```

History

Release version	Command history
8.0.30	This command was introduced.

Related Commands

show interfaces ethernet, show interfaces tunnel, show interfaces ve, show ip ospf interface, show ipv6 ospf interface, show running-config interface ethernet, show running-config interface tunnel, show running-config interface ve

banner

Defines a login banner.

Syntax

banner [**exec** | **incoming**] *banner-string*

no banner [**exec** | **incoming**] *banner-string*

banner motd { *banner-string* | **require-enter-key** }

no banner motd { *banner-string* | **require-enter-key** }

Command Default

A banner is not configured.

Parameters

exec
Sets the EXEC process creation banner; that is, the message to be displayed when you enter the Privileged EXEC mode.

incoming
Sets the incoming terminal line banner; that is, the message to be displayed on the console when a user establishes a Telnet session.

banner-string
The ASCII string indicating the banner string in the format "c banner text c" where "c" is the delimiting character.

motd
Sets the message of the day (MOTD) banner; that is, the message to be displayed on a user terminal when a Telnet CLI session is established.

require-enter-key
Requires pressing of the Enter key after the MOTD message is displayed. This requirement is disabled by default. Unless configured, you do not have to press Enter after the MOTD banner is displayed.

Modes

Global configuration mode

Usage Guidelines

The *banner-string* includes a delimiting character. You begin and end the message with this delimiting character. The delimiting character can be any character except a double-quotation mark (") and cannot appear in the banner text. The banner text can be up to 4000 characters long, and can consist of multiple lines.

The **no** form of the command removes the banner. Use the **no banner motd require-enter-key** command to remove the requirement of pressing the Enter key once the banner text is displayed.

Examples

The following example shows how to set a banner with "c" as the delimiting character.

```
device(config)# banner c Good Morning! c
```

The following example shows how to set a MOTD banner with "$" as the delimiting character.

```
device(config)# banner motd $ Welcome!!! $
```

The following example shows how to configure the requirement to press the Enter key after the banner message is displayed.

```
device(config)# banner motd require-enter-key
```

The following example shows the message displayed when the requirement to press the Enter key is enabled upon accessing the switch from Telnet.

```
Authorized Access Only ...
Press <Enter> to accept and continue the login process....
```

bgp-redistribute-internal

Causes the device to allow the redistribution of IBGP routes from BGP into OSPF for non-default VRF instances.

Syntax

bgp-redistribute-internal

no bgp-redistribute-internal

Command Default

This feature is disabled.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

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.

Examples

This example enables BGP4 route redistribution.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# bgp-redistribute-internal
```

This example enables BGP4+ route redistribution in BGP address-family IPv6 unicast configuration mode.

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

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

block

Configures the time users must wait before the next cycle of Web Authentication begins after they have exceeded the limit for Web Authentication attempts.

Syntax

block [**mac** *mac-address*] **duration** *time*

no block [**mac** *mac-address*] **duration** *time*

Command Default

The default is 90 seconds.

Parameters

mac *mac-address*

Configures the host with the specified MAC address to be temporarily or permanently blocked from attempting Web Authentication.

duration *time*

Configures the time duration users must wait before the next cycle of Web Authentication attempts is allowed. Valid values are from 0 through 128,000 seconds. The default is 90 seconds, and entering 0 means the user is infinitely blocked.

Modes

Web Authentication configuration mode

Usage Guidelines

To unblock the MAC address, wait until the block duration timer expires or enter the **clear webauth vlan** *vlan-id* **block-mac** command.

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

Examples

The following example configures the block duration to 1000 seconds.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# block duration 1000
```

The following example configures the block duration for a specific host.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# block mac 1111.2222.3333 duration 1000
```

block-applicant

Disables the VLAN advertising on a GVRP-enabled port.

Syntax

block-applicant { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no block-applicant { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

VLANs are advertised on GVRP-enabled ports.

Parameters

all

Disables VLAN advertising on all GVRP-enabled ports.

ethernet *stackid/slot/port*

Disables VLAN advertisement on the specified GVRP-enabled Ethernet port.

to *stackid/slot/port*

Specifies the range of GVRP-enabled Ethernet ports on which you want to disable VLAN advertising.

Modes

GVRP configuration mode

Usage Guidelines

NOTE
Even when VLAN adverstising is disabled, Leaveall messages are still sent on the GVRP ports.

The **no** form of the command allows the VLAN advertising on GVRP-enabled ports.

Examples

The following example shows how to disable VLAN advertising on all ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-applicant all
```

The following example shows how to disable VLAN advertising on specific ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-applicant ethernet 1/1/24 ethernet 1/6/24 ethernet 1/8/17
```

The following example shows how to disable VLAN advertising on a range of ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-applicant ethernet 1/1/1 to 1/1/8
```

The following example shows how to disable VLAN advertising on a list of specific ports as well as on a range of ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-applicant ethernet 1/1/1 to 1/1/8 ethernet 1/1/24 ethernet 1/6/24 ethernet
1/8/17
```

block-learning

Disables the VLAN learning on GVRP-enabled ports.

Syntax

block-learning { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no block-learning { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

VLAN learning is enabled.

Parameters

all

Disables VLAN learning on all GVRP-enabled ports.

ethernet *stackid/slot/port*

Disables VLAN learning on the specified Ethernet interface.

to *stackid/slot/port*

Specifies a range of GVRP-enabled Ethernet ports on which you want to disable VLAN learning.

Modes

GVRP configuration mode

Usage Guidelines

NOTE
The port still advertises VLAN information unless you also disable VLAN advertising.

The **no** form of the command re-enables VLAN learning.

Examples

The following example shows how to disable VLAN learning on all GVRP-enabled ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-learning all
```

The following example shows how to disable VLAN learning on a list of specific GVRP-enabled ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-learning ethernet 1/1/24 ethernet 1/6/22 ethernet 1/8/17
```

The following example shows how to disable VLAN learning on a range of GVRP-enabled ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-learning ethernet 1/1/1 to 1/1/8
```

The following example shows how to disable VLAN learning on a list of ports along with a range of GVRP-enabled ports.

```
device(config)# gvrp-enable
device(config-gvrp)# block-learning ethernet 1/1/1 to 1/1/8 ethernet 1/1/24 ethernet 1/6/24 ethernet
1/8/17
```

bootfile

Specifies the boot image to be used by the client.

Syntax

bootfile *name*

Parameters

name

Specifies the name of the bootfile to be used by the client.

Modes

DHCP server pool configuration mode

Examples

The following example specifies the bootfile name.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# bootfile foxhound
```

bootp-relay-max-hops

Modifies the maximum number of BootP or DHCP hops.

Syntax

bootp-relay-max-hops *max-hop*

no bootp-relay-max-hops *max-hop*

Command Default

By default, a Brocade Layer 3 switch forwards a BootP or DHCP request if its hop count is four or less, but discards the request if the hop count is greater than four.

Parameters

max-hop

Specifies the maximum number of hops. The parameter value can be from 1 through 15.

Modes

Global configuration mode

Usage Guidelines

This command allows the Layer 3 switch to forward BootP or DHCP requests that have passed through 10 previous hops before reaching the Layer 3 switch. Requests that have traversed 11 hops before reaching the switch are dropped. Because the hop count value initializes at zero, the hop count value of an ingressing DHCP Request packet is the number of Layer 3 routers that the packet has already traversed.

Examples

The following example modifies the maximum number of BootP or DHCP hops to 10.

```
device(config)# bootp-relay-max-hops 10
```

boot system flash

Configures the device to boot from the image stored in the flash memory.

Syntax

boot system flash { **primary** | **secondary** } [**yes**]

no boot system flash { **primary** | **secondary** } [**yes**]

Command Default

By default, the device first attempts to boot from the image stored in its primary flash, then its secondary flash, and then from a TFTP server.

Parameters

primary

Configures to boot from the image stored in its primary flash.

secondary

Configures to boot from the image stored in its secondary flash.

yes

Confirms the system boot preference settings. This option is equivalent to using the **write memory** command. This option is available only in Privileged EXEC mode.

Modes

Privileged EXEC mode

Global configuration mode

Usage Guidelines

You can use boot commands to immediately initiate software boots from a software image stored in the primary or secondary flash on a Brocade device.

It is very important that you verify a successful transfer of the boot code before you reset the system. If the boot code is not transferred successfully but you try to reset the system, the system will not have the boot code with which to successfully boot.

You can modify the default booting sequence in the global configuration mode using the **boot system** command.

Execute the **write memory** command to save the boot preferences to the startup configuration. If you are executing the **boot system flash** command from the Privileged EXEC mode, you can use the **yes** option to save the boot preference to the startup configuration. Executing the **write memory** command is not required in this case.

NOTE
FSX, ICX 6430, and ICX 6450 devices support only one configured system boot preference.

You can use the **show boot-preference** command to view the boot sequence preference.

The **no** form of the command resets the boot preference to the default.

Examples

The following example shows how to set the system to boot the image from the secondary flash.

```
device(config)# boot system flash secondary
```

The following example shows how to set the system to boot the image from the primary flash and save the preference to the startup configuration.

```
device# boot system flash primary yes
```

boot system tftp

Configures the device to boot from the image stored on a TFTP server.

Syntax

boot system tftp *server-ip file-name* [**fiber-port**]

no boot system tftp *server-ip file-name* [**fiber-port**]

Command Default

By default, the device first attempts to boot from the image stored in its primary flash, then its secondary flash, and then from a TFTP server.

Parameters

server-ip
The IP address of the TFTP server. The IP address of the device and the TFTP server should be in the same subnet.

file-name
The boot code file name.

fiber-port
Configures to boot the device from a TFTP server through the fiber connection. This option is available only in devices running router images and in Privilege EXEC mode.

Modes

Privileged EXEC mode

Global configuration mode

Usage Guidelines

It is very important that you verify a successful transfer of the boot code before you reset the system. If the boot code is not transferred successfully but you try to reset the system, the system will not have the boot code with which to successfully boot.

In FSX Series devices, the **boot system tftp** command is supported on ports Ethernet 1 through Ethernet 12 only.

The **boot system tftp** command is not supported in a stacking environment.

The **no** form of the command resets the boot preference to the default.

Examples

The following example shows how to configure the device to boot from the image stored on a TFTP server.

```
device# boot system tftp 192.168.10.1 FCXR08000.bin
```

bpdu-flood-enable

Configures the MCT cluster devices to flood the SSTP or MSTP BPDUs in the SSTPor MSTP domain.

Syntax

bpdu-flood-enable

no bpdu-flood-enable

Command Default

BPDU flooding is not enabled.

Modes

Global configuration mode

Usage Guidelines

When **bpdu-flood-enable** is configured, there should not be any links other than the ICL connecting the two MCT cluster devices. If there is an additional link, then the flooded BPDU will cause a loop and high CPU utilization.

NOTE
The **bpdu-flood-enable** command is not supported on the Brocade ICX 7750.

The **no** form of the command disables the BPDU flooding.

Examples

The following example shows how to configure BPDU flooding on the device.

```
device(config)# bpdu-flood-enable
Warning - Any recieved untagged BPDUs will now be flooded to all the ports.
```

breakout ethernet

Configures sub-ports from 40 Gbps ports.

Syntax

breakout ethernet *unit/slot/port*

breakout ethernet *unit/slot/port* **to ethernet** *unit/slot/port*

breakout ethernet *unit/slot/port* **ethernet** *unit/slot/port*

no breakout ethernet *unit/slot/port*

no breakout ethernet *unit/slot/port* **to ethernet** *unit/slot/port*

no breakout ethernet *unit/slot/port* **ethernet** *unit/slot/port*

Command Default

By default, ports that can be broken out are configured as 40 Gbps ports.

Parameters

ethernet

Specifies the connection as ethernet.

unit/slot/port

Specifies the port to be broken into 10 Gbps sub-ports. If there are two port identifiers in the command line, the first port designates the beginning port in a range of ports to be broken out, and the second port indicates the end of the breakout range. When a range is specified, the 10 Gbps sub-ports within the range are implicitly included.

to

Designates a range of ports to be configured when followed by an ending port identifier. This is an optional keyword.

Modes

Global configuration mode.

Usage Guidelines

Use the **no** form of the command to remove breakout configuration from the designated port or range of ports.

No configuration may be present on a port for which the **breakout ethernet** command is issued. When the command is issued on a port with pre-existing configuration, an error message is returned. The existing configuration must be removed before the **breakout ethernet** command is re-issued.

The **breakout ethernet** command is available only on certain ICX 7750 40 Gbps ports. Refer to the *FastIron Ethernet Switch Administration Guide* for a table of available breakout ports. Refer to the *ICX 7750 Ethernet Switch Hardware Installation Guide* for detailed information on breakout cables.

The **breakout ethernet** command can be issued on stand-alone units only. Stacking cannot be enabled on a port configured for breakout. An error is returned if you try to enable stacking on a unit that has any breakout ports configured. The breakout configuration must be removed manually before stacking can be enabled. Use the **show breakout** command to display the breakout configuration for a unit.

The **breakout ethernet** and **no breakout ethernet** commands must be followed by a **write memory** command and a **reload** command for the port configuration changes to take effect.

Examples

The following example configures breakout on port 1/1/5, after existing configuration on the port is removed.

```
Device# configure terminal
Device(config)# breakout ethernet 1/1/5
Error: Port 1/1/5 has sflow forwarding
Device(config)# interface ethernet 1/1/5
Device(config-if-e40000-1/1/5)# no sflow forwarding
Device(config-if-e40000-1/1/5)# end
Device# write memory
Write startup-config done.
Device# configure terminal
Device(config)# breakout ethernet 1/1/5
Reload required.  Please write memory and then reload or power cycle.
Device(config)# write memory
Write startup-config done.
Device(config)# Flash Memory Write (8192 bytes per dot) .
Copy Done.
Device(config)# end
Device# reload
```

The following example checks for ports with active breakout configuration and then removes breakout from ports 1/3/1 through 1/3/6.

```
Device# show breakout

Unit-Id: 1

Port       Module Exist    Module Conf     breakout_conf   breakout_oper
1/1/5      Yes             No              Yes             Yes
1/1/6      Yes             No              Yes             Yes
1/1/7      Yes             No              Yes             Yes
1/1/8      Yes             No              Yes             Yes
1/1/9      Yes             No              Yes             Yes
1/1/10     Yes             No              Yes             Yes
1/1/11     Yes             No              Yes             Yes
1/1/12     Yes             No              Yes             Yes
1/1/13     Yes             No              Yes             Yes
1/1/14     Yes             No              Yes             Yes
1/1/15     Yes             No              Yes             Yes
1/1/16     Yes             No              Yes             Yes
1/2/1      Yes             No              Yes             Yes
1/2/2      Yes             No              Yes             Yes
1/2/3      Yes             No              Yes             Yes
1/2/4      Yes             No              Yes             Yes
1/2/5      Yes             No              Yes             Yes
1/2/6      Yes             No              Yes             Yes
1/3/1      Yes             No              Yes             Yes
1/3/2      Yes             No              Yes             Yes
1/3/3      Yes             No              Yes             Yes
1/3/4      Yes             No              Yes             Yes
1/3/5      Yes             No              Yes             Yes
1/3/6      Yes             No              Yes             Yes

Device# configure terminal
Device(config)# no breakout ethernet 1/3/1 to 1/3/6
Reload required.  Please write memory and then reload or power cycle.
Device(config)# write memory
Write startup-config done.

Device(config)# Flash Memory Write (8192 bytes per dot) .
Copy Done.
Device(config)# end
Device# reload
```

NOTE

If there had been any configuration on any sub-ports (1/3/1:1 to 1/3/6:4), the **no breakout** command would have returned an error. The configuration would then have to be removed from the sub-ports before breakout configuration could be removed.

History

Release version	Command history
FastIron Release 08.0.30	This command was introduced.

bridged-routed

Changes a router ACL into an ACL applied to bridged or routed IP traffic.

Syntax

bridged-routed

no bridged-routed

Command Default

ACL support for switched traffic is disabled.

Modes

IP access list configuration mode

Usage Guidelines

The **bridged-routed** command applies to FSX devices only. For Brocade FCX Series and ICX devices, ACL support for switched traffic in the router image is enabled by default. There is no command to enable or disable it. For outbound traffic, ACL support is enabled on switched traffic by default. The **bridged-routed** command is not applicable.

To display the configuration for ACL support for switched traffic, use the **show ip access-list** command

You can use the **bridged-routed** command in conjunction with the **enable acl-per-port-per-vlan** command, to assign an ACL to certain ports of a VLAN under the virtual interface configuration level. In this case, all of the Layer 3 traffic (bridged and routed) is filtered by the ACL.

The **no** form of the command disables the ACL support for switched traffic.

Examples

The following example enables ACL support for switched traffic.

```
device(config)# ip access-list extended 111
device(config-ext-nacl)# bridged-routed
```

broadcast client

Configures a device to receive Network Time Protocol (NTP) broadcast messages on a specified interface.

Syntax

broadcast client

no broadcast client

Command Default

The broadcast mode is not enabled.

Modes

NTP interface configuration mode

Usage Guidelines

NTP broadcast client can be enabled on maximum of 16 ethernet interfaces. If the interface is operationally down or NTP is disabled, then the NTP broadcast server packets are not received.

The **no** form of the command disables the capability of a device to receive NTP broadcast messages.

Examples

The following example shows how to configure a device to receive Network Time Protocol (NTP) broadcast messages on a specified interface.

```
device(config)# ntp
device(config-ntp)# ntp-interface management 1
Brocade(config-ntp-mgmt-1)# broadcast client
```

broadcast destination

Configures NTP broadcast destination options.

Syntax

broadcast destination *ip-address* [**key** *key-id*] [**version** *version-number*]

no broadcast destination *ip-address* [**key** *key-id*] [**version** *version-number*]

Command Default

The broadcast mode is not enabled.

Parameters

ip-address

Specifies the IPv4 subnet address of the device to send NTP broadcast messages.

key *key-id*

Specifies the authentication key ID. By default, no authentication key is configured. Valid values are 1 to 65535.

version *version-number*

Specifies the Network Time Protocol (NTP) version number. The default value is 4. The version options are 3 and 4.

Modes

NTP interface configuration mode

Usage Guidelines

The NTP broadcast server can be enabled on maximum 16 ethernet interfaces and four subnet addresses per interface. If the interface is operationally down or there is no IP address configured for the subnet address, then the NTP broadcast server packets are not sent.

NOTE
This command is not effective, if the NTP server is disabled.

The **no** form of the command disables the broadcast option.

Examples

The following example shows how to configure NTP broadcast destination commands.

```
device(config)# ntp
device(config-ntp)# ntp-interface management 1
device(config-ntp-mgmt-1)# broadcast destination 10.20.99.0 key 2 version 3
```

broadcast limit

Enables rate limiting on a port, enables Syslog logging of broadcast packets, or sets a packet drop threshold value.

Syntax

broadcast limit *num* **kbps** [**log** | **threshold** *packet_threshold* **action port-shutdown** [*shutdown_seconds*]]

no broadcast limit *num* **kbps** [**log** | **threshold** *packet_threshold* **action port-shutdown** [*shutdown_seconds*]]

Command Default

Broadcast rate limiting, logging, and port dampening are disabled.

Parameters

num

Specifies the maximum number of broadcast packets per second ranging from 1 to 8388607; or when followed by **kbps**, *num* is the number of kilo bits per second (kbps) permitted for byte-based limiting. The value in this case is 1 to the maximum port speed. Use 0 to disable rate limiting.

kbps

When kbps follows num it enables byte-based limiting.

log

Enables Syslog logging when the broadcast limit exceeds *num* **kpbs** .

threshold

The packet drop count threshold.

packet_threshold

Specifies the number of packets (in kilo bytes) that when exceeded, the port is shutdown. The value ranges from 1 KB to 10 GB.

action

The action to be taken.

port-shutdown

Set the **action** as a port shutdown event.

shutdown_seconds

The amount of time, in seconds, the port is shutdown. The default is 300 seconds and the range is from 1 to 65535 seconds.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to disable rate limiting on a port, Syslog logging of excess packets, or the packet drop threshold value.

If the port *shutdown_seconds* parameter is set to 0, the port is kept in ERR-DISABLE state until you re-enabled it.

Examples

The following example enables a broadcast rate limit of 131072 kbps.

```
device(config)# interface ethernet 9/1/1
device(config-if-e1000-9/1/1)# broadcast limit 131072 kbps
```

The following example enables broadcast limit logging when the configured broadcast limit exceeds 100 Kbps.

```
device(config)# interface ethernet 1/2/1
device(config-if-e10000-1/2/1)# broadcast limit 100 kbps log
```

The following example shuts down the port for 300 seconds (default) when the packet drop threshold value exceeds 1000 KBs.

```
device(config)# interface ethernet 1/2/1
device(config-if-e10000-1/2/1)# broadcast limit 100 kbps threshold 1000 action port-shutdown
```

History

Release version	Command history
8.0.10	The command was introduced.
8.0.30h	The command was modified to include the keyword **threshold**.
8.0.40a	The command was modified to include the keyword **log**.

bsr-candidate

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

Syntax

bsr-candidate ethernet *stackid/slot/portnum hash-mask-length* [*priority*]

bsr-candidate loopback *num hash-mask-length* [*priority*]

bsr-candidate ve *num hash-mask-length* [*priority*]

bsr-candidate tunnel *num hash-mask-length* [*priority*]

no bsr-candidate

Command Default

The PIM router does not participate in BSR election.

Parameters

ethernet *stackid/slot/portnum*

Specifies the physical interface for the candidate BSR. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *num*

Specifies the loopback interface for the candidate BSR.

ve *num*

Specifies the virtual interface for the candidate BSR.

tunnel *num*

Specifies a GRE tunnel interface.

hash-mask-length

Specifies the number of bits in a group address that are significant when calculating the group-to-RP mapping. The range is 1 to 32.

NOTE
It is recommended that you specify 30 for IPv4 networks.

priority

Specifies the BSR priority. The range is from 0 to 255, from low to high. The default is 0.

Modes

PIM Router configuration mode

Usage Guidelines

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

Each PIM Sparse domain has one active BSR. For redundancy, you can configure ports on multiple devices as candidate BSRs. The PIM Sparse protocol uses an election process to select one of the candidate BSRs as the BSR for the domain. The BSR with the highest BSR priority is elected. If the priorities result in a tie, the candidate BSR interface with the highest IP address is elected.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

Examples

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

```
device(config)# router pim
Device(config-pim-router)# bsr-candidate ethernet 1/2/2 30 255
```

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

```
device(config)# router pim
device(config-pim-router)# bsr-candidate loopback 1 30 240
```

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

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

History

Release version	Command history
8.0.20	This command was modified to add the **tunnel** keyword.

buffer-profile port-region

Configures buffer profile on a device.

Syntax

buffer-profile port-region *port-region* **qd-buffer-profile** *user-profile-name*

no buffer-profile port-region *port-region* **qd-buffer-profile** *user-pr ofile-name*

buffer-profile port-region *port-region* **scheduler-profile** *user-profile-name*

no buffer-profile port-region *port-region* **scheduler-profile** *user-profile-name*

buffer-profile port-region *port-region* **voip downlink 100 uplink 1000**

no buffer-profile port-region *port-region* **voip downlink 100 uplink 1000**

Command Default

Buffer profiles are not configured.

Parameters

port-region
: Specifies the device number on which the user-configurable buffer profile is applied. The port-region number can be either 0 to 15.

qd-buffer-profile *user-profile-name*
: Applies the user defined buffer profile.

scheduler-profile*user-profile-name*
: Configures the defined scheduler profile.

voip
: Configures VoIP buffer profile.

uplink 100
: Configures the uplink ports as 100M.

downlink 1000
: Configures the downlink ports as 1000M.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command deletes the existing buffer profile configuration.

Examples

The following example shows how to apply the buffer profile named "profile1" to a device.

```
device(config)# buffer-profile port-region 0 qd-buffer-profile profile1
```

buffer-sharing-full

Removes the buffer allocation limits on all ports and all traffic classes globally.

Syntax

buffer-sharing-full

Modes

Global configuration mode

Usage Guidelines

The **buffer-sharing-full** command sets the total transmit queue depth limit and the transmit queue depth limits for each traffic class to 4095 for all ports of the device. The command overrides any existing individually configured queue depth limits. The command permits all available buffers in a port region to be used on a first-come, first-served basis by any of its ports, regardless of priority.

NOTE
The **buffer-sharing-full** command should be used carefully. By entering this command, there is no limit on the number of buffers a port or a specific priority on a port can use. One port could potentially use up all the available buffers of its port region and cause starvation on other ports of the port region. The command can create unpredictable behavior during traffic congestion or a blocking scenario, compromising network stability (by losing control packets), QoS, and stacking.

Examples

The following example removes the buffer allocation limits on all ports and all traffic classes globally.

```
device(config)# buffer-sharing-full
```

capability as4

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

Syntax

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

no capability as4 { **disable** | **enable** }

Command Default

This feature is disabled.

Parameters

disable

Disables 4-byte ASN capability at the BGP global level.

enable

Enables 4-byte ASN capability at the BGP global level.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

To enable 4-byte ASN capability:

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

captive-portal

Creates a user-defined Captive Portal profile.

Syntax

captive-portal *profile-name*

no captive-portal *profile-name*

Parameters

profile-name

Specifies the name of the user-defined Captive Portal profile.

Modes

Global configuration mode

Usage Guidelines

The Captive Portal profile serves as a template that includes configuration details specific to the external web server, such as virtual IP address, HTTP or HTTPS protocol port number, and login-page details hosted on the external captive portal server.

The details configured in the Captive Portal profile enable the switch to handle HTTP redirection mechanism and redirects the client to the login page hosted on the external captive portal server.

The Captive Portal profile can be attached to an external Web Authentication-enabled VLAN using the **captive-portal profile** command.

The **no** form of the command removes the Captive Portal profile.

Examples

The following example creates the user-defined Captive Portal profile cp_brocade.

```
device(config)# captive-portal cp_brocade
```

History

Release version	Command history
8.0.40	This command was introduced.
8.0.30j	This command was added to FastIron 8.0.30j

captive-portal profile

Applies a configured Captive Portal profile on a Web Authentication-enabled VLAN.

Syntax

captive-portal profile *profile-name*

no captive-portal profile *profile-name*

Command Default

A Captive Portal profile is not applied on a Web Authentication-enabled VLAN.

Parameters

profile-name

Specifies the Captive Portal profile to be applied on a Web Authentication-enabled VLAN.

Modes

Web Authentication configuration mode

Usage Guidelines

The **no** form of the command removes the Captive Portal profile from the Web Authentication-enabled VLAN.

Examples

The following example binds the Captive Portal profile cp_brocade on Web Authentication-enabled VLAN 10.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# captive-portal profile cp_brocade
```

History

Release version	Command history
8.0.40	This command was introduced.
8.0.30j	This command was added to FastIron 8.0.30j

cdp enable

Enables Cisco Discovery Protocol (CDP) at the interface level.

Syntax

cdp enable

no cdp enable

Command Default

CDP is not enabled. CDP is enabled on an interface once CDP is enabled on the device.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables CDP on an interface.

Examples

The following example enables CDP on an interface.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# cdp enable
```

cdp run

Enables the device to intercept and display Cisco Discovery Protocol (CDP).

Syntax

cdp run

no cdp run

Command Default

CDP is disabled by default.

Modes

Global configuration mode

Usage Guidelines

The command enables the device to detect CDP power requirements as well.

The **no** form of the command disables the device to intercept and display CDP.

Examples

The following example shows how to enable the device to intercept and display CDP.

```
device(config)# cdp run
```

chassis name

Configures chassis name.

Syntax

chassis name *name*

no chassis name *name*

Command Default

Chassis name is not configured.

Parameters

name

Specifies the name of the chassis.

Modes

Global configuration mode

Usage Guidelines

The command does not change the CLI prompt. Instead, the command assigns an administrative ID to the device.

The **no** form of the command removes the chassis name.

Examples

The following example shows how to configure the chassis name.

```
device(config)# chassis name ch_2
```

clear access-list

Clears ACL counters.

Syntax

clear access-list { **all** | *std-acl-num* | *ext-acl-num* }

Parameters

all

Clears all ACL counters.

std-acl-num

Clears the counter for the specified standard ACL. Valid values are from 1 through 99.

extd-acl-num

Clears the counter for the specified extended ACL. Valid values are from 100 through 199.

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example clears all the ACL counters.

```
device# clear access-list all
```

The following example clears the counter for the standard ACL 10.

```
device# clear access-list 10
```

clear access-list accounting

Clears Access Control List (ACL) accounting statistics for IPv4 ACLs, IPv6 ACLs, and Layer 2 MAC filters.

Syntax

clear access-list accounting all

clear access-list accounting *interface-type interface-name* **in**

clear access-list accounting traffic-policy { **all** | *name* }

Parameters

all

Clears all statistics for all ACLs.

interface-type interface-name

Specifies the ID of the Ethernet or virtual interface. Clears the accounting statistics for ACLs bound to a physical port or clears statistics for all ACLs bound to ports that are members of a virtual routing interface.

in

Clears statistics of the inbound ACLs.

traffic-policy

Clears traffic-policy statistics.

all

Clears all traffic-policy statistics.

name

Clears statistics of a specific traffic-policy.

Modes

Privileged EXEC mode

Usage Guidelines

To clear accounting statistics for all configured ACLs, use the **all** keyword.

Examples

The following example clears ACL accounting statistics for all configured ACLs.

```
device# clear access-list accounting all
```

The following example clears ACL accounting statistics for a specific port.

```
device# clear access-list accounting ethernet 1/5 in
```

The following example clears all traffic-policy statistics.

```
device#clear access-list accounting traffic-policy all
```

History

Release version	Command history
08.0.10	This command was introduced.

clear acl-on-arp

Clears the count of how many ARP packets have been dropped on the interface.

Syntax

clear acl-on-arp

Modes

Privileged EXEC mode

Global configuration mode

Usage Guidelines

The Filter Count column in the output of the **show acl-on-arp** command shows how many ARP packets have been dropped on the interface since the last time the count was cleared. The **clear acl-on-arp** command resets the filter count on all interfaces in a device back to zero.

Examples

The following example clears the count of how many ARP packets have been dropped on the interface.

```
device# clear acl-on-arp
```

clear auth-mac-table

Deletes the contents of the authenticated MAC address table.

Syntax

clear auth-mac-table [**mac-session** *mac-address* | **ethernet** *stack/slot/port* [**to** *stack/port/slot* | [**ethernet** *stack/slot/port* **to** *stack/port/slot* | **ethernet** *stack/slot/port*]...]]

Parameters

mac-session
Specifies to delete the MAC session.

mac-address
Specifies the MAC address from which the MAC sessions are to be deleted.

ethernet *slot/port*
Specifies the interface from which the MAC sessions are to be cleared.

to *slot/port*
Specifies the range of interfaces from which the MAC sessions are to be cleared.

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

dot1x authentication mode

Usage Guidelines

Use this command to delete the contents of the authenticated MAC address table either entirely, or just for the entries learned on a specified interface or range of interfaces.

Examples

The following example deletes the entire contents of the authenticated MAC address table.

```
device(config)# clear auth-mac-table
```

The following example deletes the authenticated MAC address table of entries learned on a specified interface.

```
device(config)# clear auth-mac-table ethernet 1/3
```

The following example deletes the authenticated MAC address table of entries learned on a range of interfaces.

```
device(config)# clear auth-mac-table ethernet 1/3 to 1/6
```

The following example deletes the MAC session for an address learned on a specific interface.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# clear auth-mac-table 0000.0034.abd4
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

clear cable diagnostics tdr

Clears the results of Virtual Cable Test (VCT) TDR testing (if any) conducted on the specified port

Syntax

clear cable-diagnostics tdr *stackid/slot/port*

Command Default

By default, the results of the previous test (if any) are present and are displayed in response to the **show cable-diagnostics tdr** command for the specified port.

Parameters

stackid/slot/port

Identifies the specific interface (port), by device, slot, and port number in the format shown.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear TDR test registers before every TDR cable diagnostic test. Most Brocade devices support VCT technology. VCT technology enables the diagnosis of a conductor (wire or cable) by sending a pulsed signal into the conductor, then examining the reflection of that pulse. This method of cable analysis is referred to as Time Domain Reflectometry (TDR). By examining the reflection, the Brocade device can detect and report cable statistics such as local and remote link pair, cable length, and link status.

Use the command in conjunction with the **phy cable-diagnostics tdr stackid/slot/port** command to test the interface.

Show diagnostic test results using the **show cable-diagnostics tdr stackid/slot/port** command.

This command is supported only on the Brocade ICX 6610, ICX 6430, ICX 6430-C, ICX 6450, ICX6450-C, and FCX Series devices.

Examples

In the following example, results from the previous test are cleared from the third interface on the second slot of the first device in the stack.

```
device# clear cable-diagnostics tdr 1/2/3
```

History

Release version	Command history
08.0.20	This command was introduced.

clear dhcp

Clears the DHCP binding database.

Syntax

clear dhcp *ip-address*

Parameters

ip-address

The IP address of the client.

Modes

User EXEC mode

Usage Guidelines

You can remove all entries in the database or remove entries for a specific IP address only.

Examples

The following example removes all entries from the DHCP binding database.

```
device# clear dhcp
```

The following example clears entries for a specific IP address.

```
device# clear dhcp 10.10.102.4
```

clear dot1x mac-sessions

Clears 802.1x authentication MAC sessions.

Syntax

clear dot1x mac-sessions [*mac-address* | **ethernet** *slot/port* [[**to** *slot/port*] [**ethernet** *slot/port*]...]]

Parameters

mac-address

Specifies the MAC address from which the 802.1X authentication MAC sessions are to be cleared, so that the client with that MAC address can be re-authenticated by the RADIUS server.

ethernet *slot/port*

Specifies the interface from which the 802.1X authentication MAC sessions are to be cleared.

to *slot/port*

Specifies the range of interfaces from which the 802.1X authentication MAC sessions are to be cleared.

Modes

Privileged EXEC mode

Global configuration mode

dot1x authentication mode

Examples

The following example clears the 802.1X authentication MAC session for the specified MAC address.

```
device(config)# clear dot1x mac-sessions 0000.0034.abd4
```

The following example clears the 802.1X authentication MAC sessions from an interface.

```
device(config)# clear dot1x mac-sessions ethernet 1/3
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

clear dot1x sessions

Clears 802.1X authentication sessions.

Syntax

clear dot1x sessions { *mac-address* | **ethernet** *device/slot/port* }

Parameters

mac-address

Specifies the MAC address from which the 802.1X authentication sessions are to be cleared.

ethernet *device/slot/port*

Specifies the interface from which the 802.1X authentication sessions are to be cleared.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear the 802.1X authentication sessions.

Examples

The following example clears the 802.1X authentication session for the specified MAC address.

```
device(config)# clear dot1x sessions 0000.0034.abd4
```

History

Release version	Command history
08.0.20	This command was introduced.

clear dot1x statistics

Clears 802.1X authentication statistics.

Syntax

clear dot1x statistics ethernet *unit/slot/port*

For FSX and ICX 6650 devices
clear dot1x statistics { **ethernet** *unit/slot/port* | **all** }

Parameters

ethernet *unit/slot/port*
Specifies the interface on which the 802.1X authentication statistics are to be cleared.

all
Specifies that all all 802.1X authentication statistics are to be cleared for all interfaces.

Modes

Privileged EXEC mode

Examples

The following example clears 802.1X authentication statistics.

```
device(config)# clear dot1x statistics
```

The following example clears 802.1X authentication statistics on a specific interface.

```
device(config)# clear dot1x statistics ethernet 1/1/1
```

History

Release version	Command history
08.0.20	The **all** option was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

clear dot1x statistics

Clears 802.1X authentication statistics.

Syntax

clear dot1x statistics { **ethernet** *slot/port* | **all** }

Parameters

ethernet *slot/port*

Specifies the interface on which the 802.1X authentication statistics are to be cleared.

all

Specifies that 802.1X authentication statistics are to be cleared for all interfaces.

Modes

Privileged EXEC mode

Global configuration mode

dot1x configuration mode

Examples

The following example clears 802.1X authentication statistics on all interfaces.

```
device(config)# clear dot1x statistics all
```

clear dot1x-mka statistics

Clears current MACsec Key Agreement (MKA) statistics.

Syntax

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

Parameters

ethernet *device/slot/port*

Specifies an Ethernet interface by device position in stack, slot on the device, and interface on the slot.

Modes

EXEC or Privileged EXEC mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

Examples

In the following example, MKA statistics are cleared for Ethernet interface 1/3/3 (port 3 of slot 3 on the first device in the stack).

```
device# clear dot1x-mka statistics ethernet 1/3/3
```

History

Release version	Command history
08.0.20	This command was introduced.

clear fdp counters

Clears Foundry Discovery Protocol (FDP) and Cisco Discovery Protocol (CDP) statistics.

Syntax

clear fdp counters

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

The same command clears information for both FDP and CDP.

Examples

The following example clears FDP and CDP statistics.

```
device(config)# clear fdp counters
```

clear fdp table

Clears the information received in Foundry Discovery Protocol (FDP) and Cisco Discovery Protocol (CDP) updates from neighboring devices.

Syntax

clear fdp table

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

This command clears all the updates for FDP and CDP.

Examples

The following example clears FDP and CDP updates from neighboring devices.

```
device(config)# clear fdp table
```

clear gvrp statistics

Clears statistics of the GVRP counters.

Syntax

clear gvrp statistics { **all** | **ethernet** *stackid/slot/port* }

Parameters

all

Clears the counters for all ports.

ethernet *stackid/slot/port*

Clears the counters for a specific Ethernet port.

Modes

Privileged EXEC mode

Global configuration mode

GVRP configuration mode

Examples

The following example shows how to clear statistics for all GVRP counters.

```
device# clear gvrp statistics all
```

The following example shows how to clear statistics for a specific port.

```
device# clear gvrp statistics ethernet 1/2/1
```

clear ip dhcp-server binding

Clears the leases from the lease binding database.

Syntax

clear ip dhcp-server binding { *address* | * }

Parameters

address

The IP address to be deleted.

*

Wildcard clears all lease entries.

Modes

Global configuration mode.

Usage Guidelines

Use this command to delete to delete a specific lease, or all lease entries from the lease binding database.

Examples

The following example clears all lease entries.

```
device(config)# clear ip dhcp-server binding *
```

clear ip mroute

Removes multicast routes from the IP multicast routing table .

Syntax

clear ip mroute [**vrf** *vrf-name*] [*ip-address* {*ip-mask* | *mask-bits* }]

Parameters

vrf *vrf-name*
: Specifies a VRF.

ip-address
: Specifies an IP address.

ip-mask
: Specifies an IP subnet mask.

mask-bits
: Specifies a subnet mask in bits.

Modes

Global configuration mode

Usage Guidelines

After multicast routes are cleared from an IP multicast routing table, the best static multicast routes are added back to the routing table.

When used without specifying a **vrf** *vrf-name* this command clears multicast routes from the multicast routing table.

Examples

The following example removes all mroutes from the IP multicast routing table:

```
Device# configure terminal
Device(config)# clear ip mroute
```

The following example removes all mroutes from the vrf green IP multicast routing table:

```
Device# configure terminal
Device(config)# clear ip mroute vrf green
```

The following example removes mroute 10.0.0.2/24 from the IP multicast routing table:

```
Device# configure terminal
Device(config)# clear ip mroute 10.0.0.2/24
```

History

Release version	Command history
8.0.10a	This command was introduced.

clear ip pim counters

Clears PIM message counters.

Syntax

clear ip pim [**vrf** *vrf-name*] **counters**

Parameters

vrf *vrf-name*

Specifies a VRF instance.

counters

Specifies PIM message counters.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** keyword, this command clears the PIM message counters for all VRFs.

Examples

The following example clears the PIM message counters.

```
Device# clear ip pim counters
```

The following example clears the PIM message counters on a XRF named blue.

```
Device# clear ip pim vrf blue counters
```

clear ip pim hw-resource

Clears the PIM hardware resource fail count for a specific VRF instance or for all VRFs.

Syntax

clear ip pim [**vrf** *vrf-name*] **hw-resource**

Parameters

vrf *vrf-name*

Specifies a VRF instance.

hw-resource

Specifies hardware resource fail count.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** keyword, this command clears the PIM hardware resource fail count for all VRFs.

Examples

The following example clears the PIM hardware resource fail count.

```
Device# clear ip pim hw-resource
```

clear ip pim rp-map

Updates the entries in the static multicast forwarding table for a specific VRF instance or for all VRFs.

Syntax

clear ip pim [**vrf** *vrf-name*] **rp-map**

Parameters

vrf *vrf-name*

Specifies a VRF instance.

rp-map

Specifies the entries in a PIM sparse static multicast forwarding table.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** keyword, this command clears the PIM forwarding cache for all VRFs.

Configure this command to update the entries in the static multicast forwarding table immediately after making rendezvous point (RP) configuration changes. This command is meant to be used with the **rp-address** command.

Examples

The following example clears the entries in a PIM sparse static multicast forwarding table on a VRF instance named blue.

```
Device# clear ip pim vrf blue rp-map
```

clear ip pimsm-snoop

Clears PIM sparse mode (SM) information.

Syntax

clear ip pimsm-snoop [**vlan***vlan-id*] { **cache** [*ip-address*] | **stats**}

Parameters

vlan*vlan-id*

Specifies clearing information on a specific VLAN.

cache

Specifies clearing the PIM SM snooping cache.

ip-address

Specifies clearing PIM SM snooping-cache information on a specific source or group.

stats

Specifies clearing traffic and error counters.

Modes

Global configuration mode

Examples

The following example clears PIM SM information from all VLANs.

```
Device(config)#clear ip pimsm-snoop cache
```

The following example clears PIM SM information from a specific VLAN.

```
Device(config)#clear ip pimsm-snoop vlan 10 cache
```

The following example clears PIM SM information from a specific source.

```
Device(config)#clear ip pimsm-snoop cache 10.1.1.1
```

The following example clears traffic and error counters from all VLANs.

```
Device(config)#clear ip pimsm-snoop stats
```

History

Release version	Command history
8.0.20	This command was introduced.

clear ipv6 dhcp-relay delegated-prefixes

Clears the IPv6 DHCP relay delegated prefixes.

Syntax

clear ipv6 dhcp-relay delegated-prefixes { **vrf***vrf-name* | **X:X::X:X/M** | **all** | **interface** *interface-id* }

Parameters

vrf *vrf-name*

Clears the DHCPv6 delegated prefixes for a specific VRF. If this parameter is not provided, then the information for the default VRF is cleared

X:X::X:X/M

Clears the specified delegated prefix and removes the corresponding route permanently from the router.

all

Clear all the delegated prefixes and remove the corresponding routes permanently from the router for the VRF

interface *interface-id*

Clears all the delegated prefixes and removes the corresponding routes permanently from the router for the specified outgoing interface.

Modes

Privileged EXEC mode.

Examples

The following example clears the IPv6 DHCP relay delegated prefixes from VRF1.

```
device# clear ipv6 dhcp-relay delegated-prefixes vrf VRF1
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

clear ipv6 dhcp-relay statistics

Clears the IPv6 DHCP packet counters.

Syntax

clear ipv6 dhcp-relay statistics

Modes

Privileged EXEC mode

Examples

The following example clears the IPv6 DHCP packet counters.

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

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

clear ipv6 dhcp6 snooping

Clears the IPv6 DHCP snooping database.

Syntax

clear ipv6 dhcp6 snooping *vlan*

Parameters

vlan

Specifies the VLAN.

Modes

Global configuration mode

User EXEC mode

Usage Guidelines

You can remove all entries in the database, or remove entries for a specific IP address only.

Examples

The following command clears the IPv6 entries in the database.

```
device# clear ipv6 dhcp6 snooping
```

clear ipv6 mroute

Removes IPv6 multicast routes from the IPv6 multicast routing table.

Syntax

clear ipv6 mroute [**vrf** *vrf-name*] [*ipv6-address-prefix/prefix-length*]

Parameters

vrf *vrf-name*
: Specifies a VRF route.

ipv6-address-prefix/prefix-length
: Specifies an IPv6 address prefix in hexadecimal using 16-bit values between colons as documented in RFC 2373 and a prefix length as a decimal value.

Modes

Privileged EXEC mode

Usage Guidelines

After mroutes are removed from an IPv6 multicast routing table, the best static mroutes are added back to it.

Examples

The following example removes all mroutes from the IPv6 multicast routing table:

```
Device(config)# clear ipv6 mroute
```

The following example removes all mroutes from the vrf green IPv6 multicast routing table:

```
Device(config)# clear ipv6 mroute vrf green
```

The following example removes mroute 2000:7838::/32 from the IPv6 multicast routing table:

```
Device(config)# clear ipv6 mroute 2000:7838::/32
```

History

Release version	Command history
8.0.10a	This command was introduced.

clear ipv6 neighbor

Clears the static neighbor discovery (ND) inspect entries and ND inspection statistics.

Syntax

clear ipv6 neighbor [**vrf** *vrf-name*] **inspection** [**static-entry** | **statistics**]

Parameters

vrf
: Specifies the VRF instance (optional).

vrf-name
: Specifies the ID of the VRF instance required with **vrf** .

inspection
: Specifies that the neighbor discovery messages are verified against the static ND inspection entries or dynamically learned DHCPv6 snoop entries.

static-entry
: Clears the manually configured static ND inspect entries that are used to validate the packets received on untrusted ports.

statistics
: Clears the total number of neighbor discovery messages received and the number of packets discarded after ND inspection.

Modes

Privileged EXEC mode

Global configuration mode

VRF configuration mode

Usage Guidelines

This command can be used in three different modes as shown in the examples. If used without specifying a VRF, this command clears data from the default VRF.

Examples

The following example removes the manually configured static ND inspect entries.

```
device# clear ipv6 neighbor inspection static-entry
```

The following example removes the manually configured static ND inspect entries on a VRF.

```
device# configure terminal
device(config)# vrf vrf2
device(config-vrf-vrf2)# clear ipv6 neighbor vrf vrf2 inspection static-entry
```

The following example deletes the ND inspection statistics.

```
device# configure terminal
device(config)# clear ipv6 neighbor inspection statistics
```

The following example deletes the ND inspection statistics on a VRF.

```
device# configure terminal
device(config)# clear ipv6 neighbor vrf vrf2 inspection statistics
```

History

Release version	Command history
08.0.20	This command was introduced.

clear ipv6 pim cache

Clears the IPv6 PIM forwarding cache.

Syntax

clear ipv6 pim [**vrf** *vrf-name*] **cache** *ipv6-address*

Parameters

vrf *vrf-name*

Specifies a VRF instance.

cache *ipv6-address*

Specifies group or address of the PIM forwarding cache to clear.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** keyword, this command clears information for all VRF instances.

Examples

This example shows how to clear the IPv6 PIM forwarding cache:

```
Device#clear ipv6 pim cache 2001:0DB8:0:1::1/120 5100::192:1:1:1
```

clear ipv6 pim counters

Clears IPv6 PIM message counters.

Syntax

clear ipv6 pim [**vrf** *vrf-name*] **counters**

Parameters

vrf *vrf-name*

Specifies a VRF instance.

counters

Specifies the IPv6 PIM message counters.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** keyword, this command clears information for all VRF instances.

Examples

Thi example shows how to clear the IPv6 PIM message counters:

```
Device#clear ipv6 pim counters
```

clear ipv6 pim hw-resource

Clears the IPv6 PIM hardware resource fail count for a specific VRF instance or for all VRFs.

Syntax

clear ipv6 pim hw-resource

Parameters

vrf *vrf-name*

Specifies a VRF instance.

hw-resource

Specifies hardware resource fail count.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** keyword, this command clears the PIM hardware resource fail count for all VRFs.

Examples

The following example clears the IPv6 PIM hardware resource fail count.

```
Device# clear ipv6 pim hw-resource
```

clear ipv6 pim rp-map

Clears the entries in an IPv6 PIM Sparse static multicast forwarding table, allowing a new rendezvous point (RP) configuration to be effective immediately.

Syntax

clear ipv6 pim [**vrf** *vrf-name*] **rp-map**

Parameters

vrf *vrf-name*
Specifies a VRF instance.

rp-map
Specifies the entries in a PIM sparse static multicast forwarding table.

Modes

Privileged EXEC mode

Usage Guidelines

Configuring this command clears and overwrites the static RP configuration. If you change the static RP configuration, the entries in the IPv6 PIM Sparse multicast forwarding table continue to use the old RP configuration until they are aged out. You can configure the **clear ipv6 pim rp-map** command to update the entries in the static multicast forwarding table immediately after making RP configuration changes.

This command is meant to be used with the **rp-address** command.

Examples

This example shows how to clear the entries in an IPv6 PIM Sparse static multicast forwarding table after you change the RP configuration:

```
Device#clear ipv6 pim rp-map
```

clear ipv6 pim traffic

Clears counters on IPv6 PIM traffic.

Syntax

clear ipv6 pim [**vrf** *vrf-name*] **traffic**

Parameters

vrf *vrf-name*

Specifies a VRF instance.

traffic

Specifies counters on IPv6 PIM traffic.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** keyword, this command clears counters for all VRF instances.

Examples

This example shows how to clear IPv6 PIM traffic counters on all VRF instances:

```
Device#clear ipv6 pim traffic
```

clear ipv6 pimsm-snoop

Clears PIM sparse mode (SM) information.

Syntax

clear ipv6 pimsm-snoop [**vlan***vlan-id*] { **cache** [*ipv6-address*] | **stats**}

Parameters

vlan*vlan-id*

Specifies clearing information on a specific VLAN.

cache

Specifies clearing the PIM SM snooping cache.

ipv6-address

Specifies clearing PIM SM snooping-cache information on a specific source or group.

stats

Specifies clearing traffic and error counters.

Modes

Global configuration mode

Examples

The following example clears PIM SM information from all VLANs.

```
Device(config)#clear ipv6 pimsm-snoop cache
```

The following example clears PIM SM information from a specific VLAN.

```
Device(config)#clear ipv6 pimsm-snoop vlan 10 cache
```

The following example clears PIM SM information from a specific source.

```
Device(config)#clear ipv6 pimsm-snoop cache ff05::100
```

The following example clears traffic and error counters from all VLANs.

```
Device(config)#clear ipv6 pimsm-snoop stats
```

History

Release version	Command history
8.0.20	This command was introduced.

clear ipv6 raguard

Resets the drop or permit packet counters for Router Advertisement (RA) guard policies.

Syntax

clear ipv6 raguard { *name* | **all** }

Parameters

name

An ASCII string indicating the name of the RA guard policy of which the packet counters must be cleared.

all

Clears the packet counters of all RA guard policies.

Modes

Global configuration mode

Usage Guidelines

To clear RA guard packet counters for all RA guard policies, use the **all** keyword. To clear the RA guard packet counters for a specific RA guard policy, specify the *name* of the policy.

Examples

The following example clears the packet count for an RA guard policy:

```
Brocade(config)# clear ipv6 raguard policy1
```

The following example clears the packet counters for all RA guard policies:

```
Brocade(config)# clear ipv6 raguard all
```

clear ipv6 tunnel

Clears statistics (reset all fields to zero) for all IPv6 tunnels or for a specific tunnel interface.

Syntax

clear ipv6 tunnel [*number*]

Parameters

number

Specifies the tunnel number.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

You can use the **show ipv6 tunnel** command to verify the command execution.

Examples

The following example clears statistics for tunnel 1.

```
device(config)# clear ipv6 tunnel 1
```

clear link-keepalive statistics

Clears the UDLD statistics.

Syntax

clear link-keepalive statistics

Modes

Privileged EXEC mode

Global configuration mode

Usage Guidelines

This command clears the Packets sent, Packets received, and Transitions counters in the **show link-keepalive ethernet** command output.

Examples

The following example shows how to clear the UDLD port statistics.

```
device# clear link-keepalive statistics
```

clear link-oam statistics

Clears EFM-OAM statistics from all EFM-OAM-enabled interfaces.

Syntax

clear link-oam statistics

Modes

Privileged EXEC mode

Global configuration mode

EFM-OAM protocol configuration mode

Examples

The following example clears EFM-OAM statistics from all EFM-OAM-enabled interfaces.

```
device(config)# clear link-oam statistics
```

History

Release version	Command history
08.0.30	This command was introduced.

clear lldp neighbors

Clears cached LLDP neighbor information.

Syntax

clear lldp neighbors [**ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }]

Parameters

ports
Clears LLDP neighbor information for ports.

all
Clears LLDP neighbor information for all LLDP capable ports.

ethernet *stackid/slot/port*
Clears LLDP neighbor information for the specified Ethernet interface.

to *stackid/slot/port*
Clears LLDP neighbor information for a range of Ethernet interfaces.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

The device clears cached LLDP neighbor information after a port becomes disabled and the LLDP neighbor information ages out. However, if a port is disabled and then re-enabled before the neighbor information ages out, the device will clear the cached LLDP neighbor information when the port is re-enabled.

Examples

The following example clears the cached LLDP neighbor information for a specific port.

```
device# clear lldp neighbors ports ethernet 1/1/10
```

The following example clears the cached LLDP neighbor information for all ports.

```
device# clear lldp neighbors ports all
```

clear lldp statistics

Clears the global and per-port LLDP neighbor statistics on the device.

Syntax

clear lldp statistics [**all** | **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }]

Parameters

all
Clears LLDP neighbor neighbor statistics information for all LLDP capable ports.

ports
Clears LLDP neighbor statistics for ports.

all
Clears LLDP neighbor statistics for all ports.

ethernet *stackid/slot/port*
Clears LLDP neighbor statistics information for the specified Ethernet interface.

to *stackid/slot/port*
Clears LLDP neighbor statistics information for a range of Ethernet interfaces.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example clears the LLDP neighbor statistics information for all the ports.

```
device# clear lldp statistics ports all
```

clear logging

Clears the log entries from the dynamic buffer, static buffer or the local buffer.

Syntax

clear logging [**dynamic-buffer** | **static-buffer**]

Parameters

dynamic-buffer
Clears dynamic buffer.

static-buffer
Clears static buffer.

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example clears the syslog messages stored in the local buffer.

```
device# clear logging
```

The following example clears the dynamic buffer.

```
device# clear logging dynamic-buffer
```

clear loop-detection

Clears loop detection statistics and enables all Err-Disabled ports.

Syntax

clear loop-detection

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example clears loop detection statistics and enables all Err-Disabled ports.

```
device(config)# clear loop-detection
```

clear mac-address

Clears the MAC addresses.

Syntax

clear mac-address [*mac-address* | **ethernet** *slot/port* | **vlan** *vlan-id* | **mdup-stats**]

Parameters

mac-address

Clears entries in all VLANs with the specified MAC address.

ethernet *slot/port*

Clears the entries on the specfifed port.

vlan *vlan-id*

Clears all entries in a VLAN.

mdup-stats

Clears all MAC database update statistics. This option is available only on FSX devices.

Modes

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

Examples

The following example shows how to clear the MAC address of a specific VLAN.

```
device# clear mac-address vlan 2
```

The following example shows how to clear all MAC addresses in the system.

```
device# clear mac-address
```

clear mac-address cluster

Clears cluster-specific MAC addresses.

Syntax

clear mac-address cluster { *cluster-name* | *cluster-id* } [**vlan** *vlan-id*] [**client** [*client-name*]] [**local** | **remote**]

Parameters

cluster-name
: Clears the cluster MAC address entries for the cluster identified by the cluster name.

cluster-id
: Clears the cluster MAC address entries for the cluster identified by the cluster ID.

vlan *vlan-id*
: Clears the VLAN ID for which you want to clear the MAC address.

client *client-name*
: Clears cluster client MAC address entries.

local
: Clears the MAC addresses local to the cluster.

remote
: Clears the MAC addressses remote to the cluster.

Modes

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

Usage Guidelines

The **clear mac-address cluster** command is available only on FSX devices.

Examples

The following example shows how to clear cluster-specific MAC addresses.

```
device# clear mac-address cluster AGG-1 local
```

The following example shows how to clear a MAC address for cluster client for a specific VLAN ID.

```
device# clear mac-address cluster AGG-1 vlan 1 local
```

The following example shows how to clear MAC address for cluster client.

```
device# clear mac-address cluster AGG-1 vlan 2 client 1 local
```

clear mac-authentication sessions

Clears MAC authentication sessions.

Syntax

clear mac-authentication sessions { **mac-address** *mac-address* | **ethernet** *device/slot/port* }

Parameters

mac-address

Specifies the mac-address from which the MAC authentication sessions are to be cleared.

ethernet *device/slot/port*

Specifies the interface from which the MAC authentication sessions are to be cleared.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear the MAC authentication sessions for either a specified MAC address or an ethernet interface.

Examples

The following example clears the MAC authentication session for the specified MAC address.

```
device# clear mac-authentication sessions 0000.0034.abd4
```

The following example clears the MAC authentication session sessions on an interface.

```
device# clear mac-authentication sessions ethernet 1/1/1
```

The following example clears the MAC authentication sessions.

```
device# clear mac-authentication sessions
```

History

Release version	Command history
08.0.20	This command was introduced.

clear macsec ethernet

Clears the MACsec traffic statistics for the specified interface.

Syntax

clear macsec ethernet *device/slot/port*

Parameters

device/slot/port

Specifies an interface by device position in stack, slot on the device, and interface on the slot.

Modes

Privileged EXEC mode.

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

Examples

In the following example, MACsec traffic statistics are cleared for interface 1/3/3 (port 3 of slot 3 on the first device in the stack).

```
device(config-dot1x-mka-1/3/3)# clear macsec ethernet 1/3/3
```

History

Release version	Command history
08.0.20	This command was introduced.

clear management-vrf-stats

Clears the management Virtual Routing and Forwarding (VRF) rejection statistics.

Syntax

clear management-vrf-stats

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface management configuration mode

Usage Guidelines

You can use the **show management-vrf** command to verify the command execution.

Examples

The following example clears the management VRF rejection statistics.

```
device(config)# clear management-vrf-stats
```

clear notification-mac statistics

Clears the MAC-notification statistics, such as the number of trap messages and number of MAC notification events sent.

Syntax

clear notification-mac statistics

Command Default

The MAC-notification statistics are available on the device.

Modes

Global configuration

Privileged EXEC

Usage Guidelines

MAC notification statistics can be viewed using the **show notification-mac** display command.

Examples

The following example clears the MAC notification statistics:

```
device(config)# clear notification-mac statistics
```

History

Release version	Command history
08.0.10	This command was introduced.

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
08.0.20	This command was introduced.

clear port security

Clears port security data.

Syntax

clear port security { **restricted-macs** | **statistics** } { **all** | **ethernet** *stack/slot/port* }

Parameters

restricted-macs
Clears all restricted MAC addresses globally.

statistics
Clears violation statistics globally.

all
Clears information for all ports.

ethernet *stack/slot/port*
Clears information for the specified Ethernet port.

Modes

Privileged EXEC mode

Global configuration mode

Port security configuration mode

Port security interface configuration mode

Examples

The following example clears all restricted MAC addresses globally.

```
device# clear port security restricted-macs all
```

The following example clears restricted MAC addresses on a specific port.

```
device# clear port security restricted-macs ethernet 1/1/1
```

The following example clears violation statistics globally.

```
device# clear port security statistics all
```

The following example clears violation statistics on a specific port.

```
device# clear port security statistics ethernet 1/1/1
```

clear public-key

Clears the authorized client public key from the buffer.

Syntax

clear public-key

Modes

Privileged EXEC mode

Global configuration mode

Examples

The following example clears the client public key from the buffer.

```
device# clear public-key
```

clear pvstplus-protect-statistics

Clears the statistics of the PVST+ Protect feature, configured by means of the **pvstplus-protect** command.

Syntax

clear pvstplus-protect-statistics [**ethernet** *unit/slot/port*]

Command Default

None

Parameters

ethernet

Specifies an Ethernet port.

unit/slot/port

Number of an Ethernet port. Ranging is allowed by means of the "to" keyword.

Modes

Privileged EXEC mode

Examples

To clear the statistics of PVST+ Protect on all Ethernet interfaces, including the number of dropped PVST+ BPDUs:

```
device# clear pvstplus-protect-statistics
```

To clear the statistics of PVST+ Protect on a single Ethernet interface:

```
device# clear pvstplus-protect-statistics ethernet 1/1/1
```

To clear the statistics of PVST+ Protect on a range of Ethernet interfaces:

```
device# clear pvstplus-protect-statistics ethernet 1/1/1 to 1/1/4
```

History

Release version	Command history
08.0.30mb	This command was introduced.

clear stack ipc

Clears stack traffic statistics.

Syntax

clear stack ipc

Command Default

Stack traffic statistics are collected and retained.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **clear stack ipc** command before issuing the **show stack ipc** command. This helps to ensure that the data are the most recent traffic statistics for the stack.

This command must be executed from the active stack controller.

Examples

The following example clears stack traffic statistics prior to using the **show stack ipc** command to display current stack traffic statistics.

```
device# clear stack ipc
device# show stack ipc
V15, G1, Recv: SkP0:3749372, P1:3756064, MAIL:184291175, sum:191796611, t=457152.2
Message types have callbacks:
1 :Reliable IPC message 2 :Reliable IPC atomic 4 :fragmentation, jumbo
5 :probe by mailbox 6 :rel-mailbox 7 :test ipc
8 :disable keep-alive 9 :register cache 10:ipc dnld stk
11:chassis operation 12:ipc stk boot 13:Rconsole IPC message
14:auth msg 15:ipc erase flash 16:unconfigure
17:ipc stk boot 18:ss set 19:sFlow IPC message
21:SYNC download reques 23:SYNC download 1 spec 28:SYNC client hello
30:SYNC dy chg error 32:active-uprintf 33:test auth msg
34:probe KA 39:unrel-mailbox 40:trunk-probe
Send message types:
[1]=2342639, [4]=44528, [5]=961830, [6]=37146,
[9]=73104634, [11]=137082, [14]=487007, [20]=2304,
[22]=1395, [25]=23, [26]=1901701, [29]=415888,
[34]=1827543, [39]=30451, [40]=289420,
Recv message types:
[1]=2016251, [4]=1352759, [5]=470884, 475144,
[6]=114459, 114572, [9]=367644144, [11]=1785229,
[14]=973285, 974177, [21]=1395, [30]=25,
[34]=912972, 914086, [39]=973492, 973440, [40]=700313,
Statistics:
send pkt num : 34068433, recv pkt num : 191796609,
send msg num : 79756048, recv msg num : 379902767,
send frag pkt num : 22264, recv frag pkt num : 493860,
pkt buf alloc : 34068433,
Reliable-mail send success receive duplic
target ID 1 1 0 0
target MAC 15230 15230 0 0
unrel target ID 7615 0
There is 1 current jumbo IPC session
Possible errors:
*** recv from non-exist unit 2 times: unit 5
```

History

Release version	Command history
08.0.00a	This command was introduced.

clear statistics

Clears all counters and statistics.

Syntax

clear statistics [**dos-attack** | **traffic-policy** *traffic-policy-name*]

clear statistics [**rate-counters**] [**ethernet** *stackid/slot/port* | **management** *number* | **tunnel** [*number*] | **unit** *number*]

Parameters

dos-attack
Clears statistics about ICMP and TCP SYN packets dropped because burst thresholds were exceeded.

traffic-policy *traffic-policy-name*
Clears traffic policy counters (access list and rate limit counters).

rate-counters
Clears the rate counters.

ethernet *stackid/slot/port*
Clears egress queue statistics (resets the statistics to zero).

management *number*
Clears all statistics on a management port.

tunnel
Clears all GRE tunnel statistics.

number
Clears GRE tunnel statistics for the specified tunnel.

unit *number*
Clears a stack unit statistics.

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example clears the statistics for a specific Ethernet interface.

```
device(config)# clear statistics ethernet 1/1/1
```

The following example clears the rate counters for a tunnel interface.

```
device(config)# clear statistics rate-counters tunnel 2
```

The following example clears the statistics about ICMP and TCP SYN packets dropped.

```
device(config)# clear statistics dos-attack
```

The following example clears access list and rate limit counters.

```
device(config)# clear statistics traffic-policy counttwo
```

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
08.0.20	This command was introduced.

clear webauth vlan

Clears the authenticated hosts or the blocked hosts.

Syntax

clear webauth vlan *vlan-id*{ **authenticated-mac** | **block-mac** } [*mac-address*]

Parameters

vlan-id

Specifies the VLAN ID.

authenticated-mac

Clears authenticated hosts in a Web Authentication VLAN. If a MAC address is specified, then only that host is cleared. If a MAC address is not specified, then all the authenticated hosts are cleared.

block-mac

Clears the configured time duration users must wait before the next cycle of Web Authentication attempts is allowed. If a MAC address is specified, then only that host is unblocked. If no MAC address is specified, then all the hosts are unblocked.

mac-address

Specifies the MAC address of the host. When used with **authenticated-mac** keyword, this is the dynamically authenticated host MAC address and when used with the **block-mac** keyword, this is the blocked host MAC address.

Modes

Privileged EXEC mode

Global configuration mode

VLAN configuration mode

Web Authentication configuration mode

Examples

The following example clears all the authenticated hosts.

```
device# clear webauth vlan 10 authenticated-mac
```

The following example clears the host with MAC address 1111.2222.3333.

```
device# clear webauth vlan 10 authenticated-mac 1111.2222.3333
```

The following example unblocks an authenticated host.

```
device# clear webauth vlan 20 block-mac 1111.2222.3333
```

clear web-connection

Clears all web management sessions.

Syntax

clear web-connection

Modes

Privileged EXEC mode

Global configuration mode

Examples

The following example shows how to clear all the web management sessions.

```
device# clear web-connection
```

clear stp-protect-statistics

Clears the BPDU drop counters for all ports on the device that have STP Protection enabled.

Syntax

clear stp-protect-statistics [**ethernet** *stackid/slot/port*]

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet interface on which to clear the BPDU drop counters.

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

For each port that has STP Protection enabled, the Brocade device counts and records the number of dropped BPDUs. You can use this command to clear the BPDU drop counters for all ports on the device, or for a specific port on the device.

Examples

The following example shows how to clear the BPDU drop counters on all ports.

```
device(config)# clear stp-protect-statistics
```

The following example shows how to clear the BPDU drop counter on a specific port.

```
device(config)# clear stp-protect-statistics ethernet 1/1/1
```

client

Configures cluster clients manually.

Syntax

client *client-name*

no client *client-name*

Command Default

Cluster clients are not configured.

Parameters

client-name

Specifies the name of the client. The client name is an ASCII string and can be up to 64 characters in length.

Modes

Cluster configuration mode

Usage Guidelines

Client configuration requires client-name, RBridge ID, and Cluster Client Edge Port (CCEP). The client name can be different on the different cluster devices.

The **no** form of the command removes the manually configured cluster client.

Examples

The following example shows how to configure the client manually.

```
device(config)# cluster SX 10
device(config-cluster-SX)# client client-2
device(config-cluster-SX-client-2)# rbridge-id 200
device(config-cluster-SX-client-2)# client-interface ethernet 1/2/8
device(config-cluster-SX-client-2)# deploy
```

client-auto-detect config

Configures the automatically detected cluster clients into the running configuration and deploys all of the automatically detected clients.

Syntax

client-auto-detect config [**deploy-all**]

no client-auto-detect config [**deploy-all**]

Command Default

The cluster clients are not automatically detected and deployed.

Parameters

deploy-all

Deploys all automatically detected cluster clients.

Modes

Cluster configuration mode

Usage Guidelines

The **no** form of the command removes the configured and deployed automatically detected cluster clients.

Examples

The following example shows how to configure the automatically detected clients into the running configuration.

```
device(config)# cluster SX 400
device(config-cluster-SX)# client-auto-detect config
```

client-auto-detect ethernet

Enables cluster client automatic configuration on a specific port or range of ports.

Syntax

client-auto-detect ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no client-auto-detect ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

Cluster client automatic configuration is not enabled on the ports.

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet port on which you want to enable the cluster client automatic configuration.

to *stackid/slot/port*

Specifies the range of ports on which you want to enable the cluster client automatic configuration.

Modes

Cluster configuration mode

Usage Guidelines

The **no** form of the command disables the cluster client automatic configuration on the ports.

Examples

The following example shows how to enable cluster client automatic configuration on an Ethernet port.

```
device(config)# cluster SX 400
device(config-cluster-SX)# client-auto-detect ethernet 1/1/15
```

The following example shows how to enable cluster client automatic configuration on a range of ports.

```
device(config)# cluster SX 400
device(config-cluster-SX)# client-auto-detect ethernet 1/1/15 to 1/1/18
```

client-auto-detect start

Starts the cluster client automatic configuration.

Syntax

client-auto-detect start [**config-deploy-all**]

Command Default

The client automatic detection process is not enabled.

Parameters

config-deploy-all

Configures and deploys all automatically detected clients.

Modes

Cluster configuration mode

Usage Guidelines

Make sure that the network connection and configuration are in place before using this command. Within one minute of the time that each client is discovered, the client is automatically configured and deployed into the running configuration.

Within one minute of configuring this command, the system reports information and errors (if there are mismatches, such as an LACP configuration mismatch). You can fix a mismatch while the process is running.

Use the **config-deploy-all** option as an alternative to the **client-auto-detect config** command. The **client-auto-detect config** command also configures automatically detected clients into the running configuration and deploys all of the automatically detected clients.

Examples

The following example shows how to start the client automatic configuration process.

```
device(config)# cluster SX 400
device(config-cluster-SX)# client-auto-detect start
```

client-auto-detect stop

Stops the automatic configuration process of the running cluster client.

Syntax

client-auto-detect stop

Command Default

The automatic configuration process of the running cluster client is not stopped if the client automatic detection process is enabled using the **client-auto-detect ethernet** command.

Modes

Cluster configuration mode

Usage Guidelines

All auto-detected but unconfigured clients will be removed.

Examples

The following example shows how to stop the automatic configuration process of the running cluster client.

```
device(config)# cluster SX 400
device(config-cluster-SX)# client-auto-detect stop
```

client-interface

Configures the physical port or static LAG port as the Cluster Client Edge Port (CCEP).

Syntax

client-interface ethernet *stackid/slot/port*

no client-interface ethernet *stackid/slot/port*

Command Default

A port is not configured as the CCEP.

Parameters

ethernet *slot/port*

Configures the specified Ethernet port as the client CCEP.

Modes

Cluster configuration mode

Cluster client configuration mode

Usage Guidelines

The **no** form of the command removes the port as the CCEP.

Examples

The following example shows how to configure a port as the CCEP.

```
device(config)# cluster SX 400
device(config-cluster-SX)# client 1
device(config-cluster-SX-client-1)# rbridge-id 200
device(config-cluster-SX-client-1)# client-interface ethernet 1/1/5
device(config-cluster-SX-client-1)# deploy
```

client-interfaces shutdown

Shuts down all the local client interfaces in the cluster.

Syntax

client-interfaces shutdown

no client-interfaces shutdown

Command Default

Client interfaces are active.

Modes

Cluster configuration mode

Usage Guidelines

Use the **client-interfaces shutdown** command when performing a hitless upgrade operation. This command can be used to shut down all the local client interfaces in the cluster, resulting in fail-over of traffic to the peer device.

The **no** form of the command removes the client interface shutdown.

Examples

The following example shows how to shut down all the client interfaces in the cluster.

```
device(config)# cluster SX 4000
device(config-cluster-SX)# client-interfaces shutdown
```

client-isolation

Isolates the client from the network when Cluster Communication Protocol (CCP) is not operational.

Syntax

client-isolation strict

no client-isolation strict

Command Default

Client isolation is in loose mode.

Parameters

strict

Specifies the strict isolation mode.

Modes

Cluster configuration mode

Usage Guidelines

In strict mode, when the CCP goes down, the interfaces on both the cluster devices are administratively shut down. In strict mode, the client is completely isolated from the network if the CCP is not operational.

In loose mode (default), when the CCP goes down, the peer device performs the master/slave negotiation. After negotiation, the slave shuts down its peer ports, whereas the master peer ports continue to forward the traffic (keep-alive VLAN configured).

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

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

The **no** form of the command sets client isolation mode back to loose mode.

Examples

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

```
device(config)# cluster SX 4000
device(config-cluster-SX)# client-isolation strict
```

client-to-client-reflection

Enables routes from one client to be reflected to other clients by the host device on which it is configured.

Syntax

client-to-client-reflection

no client-to-client-reflection

Command Default

This feature is enabled.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

The host device on which it is configured becomes the route-reflector server.

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.

Examples

This example configures client-to-client reflection on the BGP4 host device.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# client-to-client-reflection
```

This example disables client-to-client reflection on the BGP4+ host device.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# no client-to-client-reflection
```

clock

Sets the system time and date.

Syntax

clock { **summer-time** | **timezone** { **gmt** *gmt-time* | **us** *us-time* } }

no clock { **summer-time** | **timezone** { **gmt** *gmt-time* | **us** *us-time* } }

Parameters

summer-time

Specifies the summer time.

gmt *gmt-time*

Specifies the GMT time zone. The value can be one of the following: gmt+00 (United Kingdom), gmt+01 (France, Germany), gmt +02 (Eastern Europe, South Africa), gmt+03, gmt+03:30, gmt+04, gmt+04:30, gmt+05, gmt+05:30 (India), gmt+06, gmt+06:30, gmt+07, gmt+08 (China, Hong Kong, Taiwan), gmt+09 (Japan, Korea), gmt+09:30, gmt+10 (Australia), gmt+10:30, gmt+11, gmt +11:30, gmt+12, gmt-01, gmt-02, gmt-03, gmt-03:30, gmt-04, gmt-05, gmt-06, gmt-07, gmt-08, gmt-08:30, gmt-09, gmt-09:30, gmt-10, gmt-11, gmt-12.

us *us-time*

Specifies the US time zone. The value can be one of the following: alaska, aleutian, arizona, central, east-indiana, eastern, hawaii, michigan, mountain, pacific, samoa.

Modes

Global configuration mode

Examples

The following example shows how to set the system date and time.

```
device(config)# clock timezone us samoa
```

cluster

Configures a Multi-Chassis Trunking (MCT) cluster.

Syntax

cluster [*cluster-name*] *cluster-id*

no cluster [*cluster-name*] *cluster-id*

Command Default

An MCT cluster is not configured.

Parameters

cluster-name

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

cluster-id

Specifies the cluster ID. The ID value range can be from 1 through 4095.

Modes

Global configuration mode

Usage Guidelines

The *cluster-name* variable is optional; the device auto-generates *cluster-name* as CLUSTER-X when only the cluster ID is specified.

NOTE

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

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

Examples

The following example configures an MCT cluster.

```
device(config)# cluster SX 4000
device(config-cluster-SX)# rbridge-id 3
```

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

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

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

Examples

This example configures a cluster ID for the route reflector.

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

compare-routerid

Enables comparison of device IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

Syntax

compare-routerid

no compare-routerid

Modes

BGP configuration mode

Usage Guidelines

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-router)# compare-routerid
```

confederation identifier

Configures a BGP confederation identifier.

Syntax

confederation identifier *autonomous-system number*

no confederation identifier

Command Default

No BGP confederation identifier is identified.

Parameters

autonomous-system number

Specifies an autonomous system number (ASN). The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

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-router)# local-as 65220
device(config-bgp-router)# confederation identifier 100
```

confederation peers

Configures subautonomous systems to belong to a single confederation.

Syntax

confederation peers *autonomous-system number* [...*autonomous-system number*]

no confederation peers

Command Default

No BGP peers are configured to be members of a BGP confederation.

Parameters

autonomous-system number

Autonomous system (AS) numbers for BGP peers that will belong to the confederation. The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

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-router)# local-as 65020
device(config-bgp-router)# confederation identifier 100
device(config-bgp-router)# confederation peers 65520 65521 65522
```

connect

Specifies the devices to which a peripheral device connects in a mixed stack.

Syntax

connect *stack-unit/slotnum/portnum*

no connect *stack-unit/slotnum/portnum*

Parameters

stack-unit
: Specifies the stack unit ID.

slotnum
: Specifies the slot number.

portnum
: Specifies the port number in the slot. If the port is part of a trunk, specify only the first port number (the odd-numbered port) in the trunk.

Modes

Stack unit configuration mode

Usage Guidelines

The **connect** command can only be used on the ICX 6610.

The **no** form of this command removes the connection configuration.

The active controller always generates a connect for live peripheral units during stack construction.

This command is optional and can be specified only for peripheral units. You cannot override the physical connections using the **connect** command. However, you can use this command on peripheral devices to make sure that a peripheral device has the unit ID you want if a unit is replaced.

You can use this command when configuring a mixed stack with the automatic configuration method.

Examples

The following example connects stack unit 3 (a peripheral device) to stack unit 1 (the active controller) and to stack unit 4 (another peripheral device).

```
Brocade(config-unit-3)# connect 1/3/1
Brocade(config-unit-3)# connect 4/2/3
```

History

Release	Command History
08.0.00a	This command was introduced.

console timeout

Configures the idle time for a serial console session.

Syntax

console timeout *time*

no console timeout *time*

Command Default

By default, a Brocade device does not time out serial console sessions.

Parameters

time

The time a serial session can remain idle before it is timed out, in minutes. The valid range is from 0 through 240. The default value is 0 (no timeout).

Modes

Global configuration mode

Stacking configuration mode

Usage Guidelines

A serial session remains open indefinitely until you close it. You can define how many minutes a serial management session can remain idle before it is timed out.

NOTE
You must enable AAA support for console commands, AAA authentication, and EXEC authorization to set the console idle time.

NOTE
In RADIUS, the standard attribute Idle-Timeout is used to define the console session timeout value. The attribute Idle-Timeout value is specified in seconds. Within the switch, the idle-Timeout value is truncated to the nearest minute, because the switch configuration is defined in minutes.

You can also configure the console timeout (in minutes) on all stack units (including the Active Controller).

The **no** form of the command removes the timeout settings.

Examples

The following example shows how to configure the console session timeout as 10 minutes.

```
device(config)# console timeout 10
```

The following example shows how to configure the console timeout on a stack unit.

```
device(config)# stack unit 3
device(config-unit-3)# console timeout 5
```

copy disk0

Copies the license, running configuration, and startup configuration from disk0 to flash.

Syntax

copy disk0 [**license** | **running-config** | **startup-config**] *filename*

Parameters

license
Copies the software license from disk0 to flash.

running-config
Copies the running configuration from disk0 to flash.

startup-config
Copies the startup-configuration from disk0 to flash.

Modes

Privileged EXEC mode.

Usage Guidelines

Use the **show files** command to verify if the running configuration and startup configuration are copied to flash correctly. Use the **show license** command to verify if the license is copied correctly.

Examples

The following example shows copying the license from disk0 to flash.

```
device# copy disk0 license 20140611132829945ICX7450-PREM-LIC-SW.XML unit 1

Copy Software License from disk0 to Flash
```

The following example shows copying the running configuration from disk0 to flash.

```
device# copy disk0 running-config running-config
```

The following example shows copying the log file.

```
device# copy flash disk0 file ./logs/pid-log.txt pid-log-brocade
Done.
```

History

Release version	Command history
08.0.30	This command was introduced.

copy flash console

Displays the contents of a flash configuration file.

Syntax

copy flash console *filename*

Parameters

filename

Specifies the name of a file stored in the flash memory.

Modes

Privileged EXEC mode

Usage Guidelines

The **copy flash console** command can be used to display the contents of a configuration file, backup file, or renamed file stored in flash memory. The file contents are displayed on the console when the command is entered at the CLI.

To display a list of files stored in flash memory:

- For devices other than FCX and ICX, enter the **dir** command at the monitor mode.
- For FCX devices, enter the **show dir** command at any level of the CLI.
- For ICX devices, enter the **show files** command at the device configuration prompt.

Examples

The following example displays the contents of a configuration file, backup file, or renamed file stored in flash memory.

```
device# copy flash console startup-config.backup

ver 08.0.30 !
stack unit 1
module 1 fcx-24-port-management-module
module 2 fcx-cx4-2-port-16g-module
module 3 fcx-xfp-2-port-10g-module
priority 80
stack-port 1/2/1 1/2/2
stack unit 2
module 1 fcx-48-poe-port-management-module
module 2 fcx-cx4-2-port-16g-module
module 3 fcx-xfp-2-port-10g-module
stack-port 2/2/1 2/2/2
stack enable
!!!!
vlan 1 name DEFAULT-VLAN by port
no spanning-tree
metro-rings 1
metro-ring 1
master
ring-interfaces ethernet 1/1/2 ethernet 1/1/3
enable
!
vlan 10 by port
mac-vlan-permit ethe 1/1/5 to 1/1/6 ethe 2/1/5 to 2/1/6 no spanning-tree !
vlan 20 by port
untagged ethe 1/1/7 to 1/1/8
no spanning-tree
pvlan type primary
pvlan mapping 40 ethe 1/1/8
pvlan mapping 30 ethe 1/1/7
!
vlan 30 by port
untagged ethe 1/1/9 to 1/1/10
no spanning-tree
pvlan type community
!
...
some lines omitted for brevity...
```

copy flash disk0

Copies the image binary stored in primary or secondary partition of the flash to the external USB flash drive.

Syntax

copy flash disk0 { **file** | **primary** | **secondary** } *file name*

Parameters

file

Specifies the file to be copied.

primary

Specifies the primary partition of the flash where the source file is located.

secondary

Specifies the secondary partition of the flash where the source file is located.

Modes

Privileged EXEC mode.

Usage Guidelines

Use the **show files disk0** to verify the files copied.

Examples

The following example shows copying the image binary stored in the primary partition of the flash to the external USB.

```
device# copy flash disk0 primary SWR08030q040.bin
Flash Memory Write (8192 bytes per dot)
.....................................................................................................
........
Copy Done.
```

The following example shows copying the core files from the flash to disk0.

```
device# copy flash disk0 file ./cores/core_1078-1.gz   core-file

Automatic copy to member units: 1
Flash Memory Write (8192 bytes per dot) ICX7450-48
Switch#.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................
Copy Done.
```

The following example shows copying the log files from flash to disk0.

```
device# copy flash disk0 file ./logs/pid-log.txt pid-log-brocade
Done.
```

History

Release version	Command history
08.0.30	This command was introduced.

copy flash scp

Uploads a copy of an OS image file from a FastIron device's primary or secondary flash memory to an SCP server. The syntax for copying an image between two devices under test (DUTs) is different from the syntax for uploading from a Brocade device to a Linux or a Windows server.

Syntax

Syntax for copying an image between two DUTs:

copy flash scp { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-prefix/prefix-length* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { **flash:primary** | **secondary** }

Syntax for uploading from a Brocade device to a Linux or a Windows server:

copy flash scp { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-prefix/prefix-length* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { **primary** | **secondary** }

Parameters

ipv4-address-
: Specifies the IPV4 address of the SCP server.

ipv4-hostname-
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
Specifies the remote port number for the TCP connection.

remote-filename
Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

flash:primary
Specifies the binary image in primary flash memory. Configure the **flash:primary** keyword when transferring files between DUTs,. See the usage note regarding using this keyword when transferring files between DUTs.

primary
Specifies the binary image in primary flash memory.

secondary
Specifies the binary image in secondary flash memory.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

NOTE
When transferring files between DUTs, you should configure the **flash:primary** keyword instead of the **primary** keyword because the SCP server does not support remote-filename aliases.

Examples

The following example uploads a copy of an OS image file from the primary flash memory on a Brocade device to the SCP server:

```
device# copy flash scp 10.20.1.1 FCXR08011-scp.bin primary
device# copy flash scp 10.20.1.1 FCXR08011-scp.bin secondary
```

The following example uploads a copy of an OS image file from the primary flash memory on a Brocade device to an SCP server with the IP address of 172.26.51.180 :

```
device# copy flash scp 172.26.51.180 filename primary
```

The following example specifies that the SCP connection is established using SSH public key authentication:

```
device# copy flash scp 172.26.51.180 public-key dsa filename primary
```

History

Release version	Command history
08.0.20	This command was introduced.

copy flash tftp

Copies contents on the device flash memory to a TFTP server.

Syntax

copy flash tftp { *ipv4-address* | *ipv6-address* } *file-name* { **file** | **primary** | **secondary** }

Parameters

ipv4-address
: Specifies the IPv4 address of the TFTP server.

ipv6-address
: Specifies the IPv6 address of the TFTP server.

file-name
: Specifies the name of the file that must be copied from the flash memory to the TFTP server.

file
: Copies a file from flash memory to the TFTP server.

primary
: Copies the primary code image to the TFTP server.

secondary
: Copies the secondary code image to the TFTP server.

Modes

Privileged EXEC mode

Examples

The following example copies the primary code image from the device flash to the TFTP server.

```
device# copy flash tftp 192.168.10.1 kxz10100.bin primary
```

copy running-config disk0

Copies the running configuration from internal flash to external USB flash drive.

Syntax

copy running-config disk0 {**filename**}

Parameters

filename

Specifies the system's running configuration file.

Modes

Privileged EXEC.

Usage Guidelines

Use the **show files** command to verify the running configuration is copied.

Examples

The following example shows copying the running configuration from the internal flash to the external USB flash drive.

```
device# copy running-config disk0  running-config7750
```

History

Release version	Command history
08.0.30	This command was introduced.

copy running-config scp

Uploads a copy of the running configuration file from a FastIron device to an SCP server.

Syntax

copy running-config scp { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

ipv4-address
: Specifies the IPV4 address of the SCP server.

ipv4-hostname
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the remote port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is going to be uploaded. You can specify up to 127 characters for the filename.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

Examples

The following example uploads a copy of the running configuration file from a FastIron device to a 172.26.51.180 SCP server:

```
device# copy running-config scp 172.26.51.180 runConfig
```

History

Release version	Command history
08.0.20	This command was introduced.

copy running-config tftp

Uploads a copy of the running configuration file from the Layer 2 Switch or Layer 3 Switch to a TFTP server.

Syntax

copy running-config tftp *tftp-ip-addr filename*

Parameters

tftp-ip-addr

TFTP server IPv4 or IPv6 address.

filename

Specifies the file name.

Modes

Privileged EXEC mode

Examples

The following example shows how to upload a copy of the running configuration file.

```
device# copy running-config tftp 192.168.14.26 copyrun
```

copy scp flash

Downloads from an SCP server a copy of the OS image file to a FastIron's device's primary or secondary flash memory or a copy of the boot file or the signature file to the FastIron device. The syntax for copying an image between two devices under test (DUTs) is different from the syntax for downloading from a DUT to a Linux or a Windows server.

Syntax

Syntax for copying an image between two DUTs:

copy scp flash { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { { **flash:primary** | **secondary** } | **bootrom** | { **fips-primary-sig** | **fips-secondary-sig** | **fips-bootrom-sig** } } [**icx6450** | **icx6610**]

Syntax for downloading from a DUT to a Linux or a Windows server:

copy scp flash { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* { { **primary** | **secondary** } | **bootrom** | { **fips-primary-sig** | **fips-secondary-sig** | **fips-bootrom-sig** } } [**icx6450** | **icx6610**]

Parameters

ipv4-address
: Specifies the IPV4 address of the SCP server.

ipv4-hostname
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address
: Specifies the IPV6 address of the SCP server.

ipv6-hostname
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
Specifies the remote port number for the TCP connection.

remote-filename
Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

flash:primary
Specifies the binary image in primary flash memory. Configure the **flash:primary** keyword when transferring files between DUTs,. See the usage note regarding using this keyword when transferring files between DUTs.

primary
Specifies the binary image in primary flash memory. Configure the **primary** keyword when transferring files between DUTs. See the usage note regarding using this keyword when transferring files between DUTs.

secondary
Specifies the binary image in secondary flash memory.

bootrom
Specifies the boot file image in the SCP server.

fips-primary-sig
Specifies the signature filename in SCP server.

fips-secondary-sig
Specifies the signature filename in SCP server.

fips-bootrom-sig
Specifies the signature filename in SCP server.

icx6450
Specifies the FastIron ICX 6450 as the device to which the signature file is downloaded.

icx6610
Specifies the FastIron ICX 6610 as the device to which the signature file is downloaded.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

NOTE
When transferring files between DUTs, you should configure the **flash:primary** keyword instead of the **primary** keyword because the SCP server does not support remote-filename aliases.

Examples

The following example copies an image from an SCP server to a Brocade device:

```
device# copy scp flash 10.20.1.1 FCXR08011.bin primary
device# copy scp flash 10.20.1.1 FCXR08011.bin secondary
```

The following example downloads a copy of the signature file from a 172.26.51.180 SCP server to a Brocade ICX 6610 device:

```
device# copy scp flash 172.26.51.180 /tftpboot/ICX6610.sig fips-primary-sig
```

History

Release version	Command history
08.0.20	This command was introduced.

copy scp license

Downloads a copy of the license file from an SCP server to a FastIron device.

Syntax

copy scp license { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* [**unit** *unit-id*]

Parameters

ipv4-address-
: Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname-
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the local port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

unit *unit-id*
: Specifies the unit ID of the device in the stack. If two or more pizza-box devices are connected and acting as a single device, a single management ID is assigned to the stack.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

Examples

The following example downloads a copy of the license file from an SCP server to a FastIron device:

```
Device# copy scp license 172.26.21.180 /tftpboot/abc.xml unit 1
Device#
```

History

Release version	Command history
08.0.20	This command was introduced.

copy scp running-config

Downloads a copy of the running configuration file from an SCP server to a FastIron device.

Syntax

copy scp running-config { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } [**outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* }] } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename* **overwrite**

Parameters

ipv4-address
: Specifies the IPV4 address of the SCP server.

ipv4-hostname
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the remote port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

overwrite

Specifies that the FastIron device should overwrite the current configuration file with the copied file. If you do not specify the **overwrite** keyword, the device copies the downloaded file into the current running or startup configuration but does not overwrite the current configuration.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

Examples

The following example downloads a copy of the running configuration file from an SCP server to a FastIron device:

```
device# copy scp running-config 172.26.51.180 abc.cfg
```

The following example downloads a copy of the running configuration file from an SCP server to a FastIron device and overwrite the current configuration file with the copied file:

```
device# copy scp running-config 172.26.51.180 abc.cfg overwrite
```

History

Release version	Command history
08.0.20	This command was introduced.

copy scp startup-config

Downloads a copy of the startup configuration file from an SCP server to a FastIron device.

Syntax

copy scp startup-config { *ipv4-address* | *ipv4-hostname* | **ipv6** { *ipv6-address* | *ipv6-hostname* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

ipv4-address
: Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the remote port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

Examples

The following example downloads a copy of the startup configuration file from an SCP server to a FastIron device:

```
device# copy scp startup-config 172.26.51.180 abc.cfg
```

History

Release version	Command history
08.0.20	This command was introduced.

copy startup-config disk0

Copies the configuration file present on the external USB to the systems startup configuration file.

Syntax

copy startup-config disk0 { **filename** }

Parameters

filename

The system's startup configuration file.

Modes

Privileged EXEC.

Usage Guidelines

Use the **show files** command to verify the startup configuration is copied.

Examples

The following example shows copying the configuration file from the external USB to the system's startup configuration file.

```
device# copy startup-config disk0 startup-config7750
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...

Done.

Copy Done.
```

History

Release version	Command history
08.0.30	This command was introduced.

copy startup-config scp

Uploads a copy of the startup configuration file from a FastIron device to an SCP server.

Syntax

copy startup-config scp { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

ipv4-address-
: Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname-
: Specifies the IP hostname of the SCP server.

ipv6
: Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length
: Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-
: Specifies the IPv6 hostname of the SCP server.

outgoing-interface
: Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*
: Configures an Ethernet interface as the outgoing interface.

ve *ve-number*
: Configures a virtual interface (VE) as the outgoing interface.

public-key
: Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa
: Specifies DSA as the public key authentication.

rsa
: Specifies RSA as the public key authentication.

remote-port
: Specifies the remote port number for the TCP connection.

remote-filename
: Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

Examples

The following example uploads a copy of the startup configuration file from a FastIron device to a to a 172.26.51.180 SCP server:

```
device# copy startup-config scp 172.26.51.180 my_startup_file
```

History

Release version	Command history
08.0.20	This command was introduced.

copy startup-config tftp

Uploads a copy of the startup configuration file from the Layer 2 Switch or Layer 3 Switch to a TFTP server.

Syntax

copy startup-config tftp *tftp-ip-addr filename*

Parameters

tftp-ip-addr

TFTP server IPv4 or IPv6 address.

filename

Specifies the file name.

Modes

Privileged EXEC mode

Examples

The following example shows how to upload a copy of the startup configuration file.

```
device# copy startup-config tftp 2001:384de::12:14 file4
```

copy tftp flash

Downloads files from a TFTP server to the flash memory of a device.

Syntax

copy tftp flash { *ipv4-address* | *ipv6-address* } *file-name* { **bootrom** | **client-certificate** | **client-private-key** | **fips-bootrom-sig** | **fips-primary-sig** | **fips-secondary-sig** | **primary** | **secondary** | **trust-certificate** }

Parameters

ipv4-address
Specifies the IPv4 address of the TFTP server from where the file must be copied to the device.

ipv6-address
Specifies the IPv6 address of the TFTP server from where the file must be copied to the device.

file-name
Specifies the name of the file that must be copied from the TFTP server.

bootrom
Specifies that the file being copied is a boot ROM image.

client-certificate
Specifies that the file being copied is a RSA client certificate file.

client-private-key
Specifies that the file being copied is a client RSA private key file.

fips-bootrom-sig
Specifies that the file being copied is a FIPS boot signature file.

fips-primary-sig
Specifies that the file being copied is a FIPS primary signature file.

fips-secondary-sig
Specifies that the file being copied is a FIPS secondary signature file.

primary
Specifies that the file being copied is a primary image file.

secondary
Specifies that the file being copied is a secondary image file.

trust-certificate
Specifies that the file being copied is an SSL trust certificate.

Modes

Privileged EXEC mode

Usage Guidelines

If the device has 8 MB of flash memory or if you want to install a Full Layer 3 image on an FCX or FSX device, you must delete the primary and secondary image.

Brocade recommends that you use the **copy tftp flash** command to copy the boot code to the device during a maintenance window. Attempting to do so during normal networking operations may cause disruption to the network.

Examples

The following example shows how to copy a boot image from the TFTP server.

```
device# copy tftp flash 192.168.10.1 grz10100.bin bootrom
```

The following example shows how to copy an OS image to the primary flash.

```
device# copy tftp flash 192.168.10.1 FCXS08020.bin primary
```

copy tftp running-config

Loads the configuration information into the running configuration.

Syntax

copy tftp running-config *ip-addr filename* [**overwrite**]

Parameters

ip-addr

TFTP server IPv4 or IPv6 address.

filename

Specifies the file name.

overwrite

Overwrites current running configuration.

Modes

Privileged EXEC mode

Examples

The following example shows how to load the configuration information into the running configuration.

```
device# copy tftp running-config 2001:384::12:13 runningfile
```

copy tftp startup-config

Downloads a copy of the startup configuration file from a TFTP server to a Layer 2 Switch or Layer 3 Switch.

Syntax

copy tftp startup-config *tftp-ip-addr filename*

Parameters

tftp-ip-addr

TFTP server IPv4 or IPv6 address.

filename

Specifies the file name.

Modes

Privileged EXEC mode

Examples

The following example shows how to download a copy of the startup configuration file.

```
device# copy tftp startup-config 2001:384::12:13 configfile
```

cpu-limit

Configures a rate limit to control the number of CPU address messages.

Syntax

cpu-limit addr-msgs *number*

no cpu-limit addr-msgs *number*

Parameters

addr-msgs *number*

The number of address messages the CPU handles per second. The range for this rate limit is from 200 through 50,000 address messages per second.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The address learning rate limit applies to each packet processor, which means that for a system with two packet processors, each processor can send address messages to the CPU at the established rate limit.

NOTE
Actual rates of address messages in hardware may have a variance of +200 or -100.

The **no** form of the command clears the rate limit for the address messages.

Examples

The following example sets the CPU address rate limit to 200.

```
device(config)# cpu-limit addr-msgs 200
```

critical-vlan

Specifies the VLAN into which the client should be placed when the RADIUS server times out while authenticating or re-authenticating users.

Syntax

critical-vlan *vlan-id*

no critical-vlan *vlan-id*

Command Default

The client is not part of the critical VLAN.

Parameters

vlan-id

Specifies the VLAN ID of the specific critical VLAN.

Modes

Authentication configuration mode

Usage Guidelines

When critical VLAN is configured and the authentication time out action is specified as critical VLAN under the port using the **authentication timeout-action critical-vlan** command at the interface level and if RADIUS timeout happens, the client is moved to the critical VLAN and any access policies applied to the critical VLAN is applied to the client.

The VLAN which is configured as a critical VLAN must be a valid VLAN configured on the device.

The **no** form of the command disables the critical VLAN by removing the client from the VLAN.

Examples

The following example configures VLAN 20 as critical VLAN.

```
device(config)# authentication
device(config-authen)# critical-vlan 20
```

History

Release version	Command history
08.0.20	This command was introduced.

crypto key client generate

Generates the crypto client key to enable SSH2.

Syntax

crypto key client generate { **dsa** | **rsa** [**modulus** *key-size*] }

Command Default

The crypto client key is not generated and SSH2 is not enabled.

Parameters

dsa
Generates a DSA client key pair.

rsa
Generates an RSA client key pair.

modulus *key-size*
Specifies the modulus size of the RSA key pair, in bits. The valid values for the modulus size are from 1024 through 2048. The default value is 1024.

Modes

Global configuration mode

Usage Guidelines

The **dsa** keyword is optional. If you do not enter the dsa keyword, the crypto key generate command generates a DSA key pair by default.

To use the SSH client for public key authentication, you must generate SSH client authentication keys and export the public key to the SSH servers to which you want to connect.

To disable SSH, you delete all of the client keys from the device. When a client key is deleted, it is deleted from the flash memory of all management modules.

Examples

The following example shows how to generate the DSA client key pair.

```
device(config)# crypto key client generate dsa
```

The following example shows how to generate the RSA key pair.

```
device(config)# crypto key client generate rsa modulus 2014
```

crypto key client zeroize

Deletes the crypto client key pair from the flash memory.

Syntax

crypto key client zeroize { **dsa** | **rsa** }

Parameters

dsa

Deletes a DSA client key pair.

rsa

Deletes an RSA client key pair.

Modes

Global configuration mode

Usage Guidelines

To disable SSH, you delete all of the client keys from the device. When a client key is deleted, it is deleted from the flash memory of all management modules.

Examples

The following example shows how to delete the DSA client key pair.

```
device(config)# crypto key client zeroize dsa
```

The following example shows how to delete the RSA client key pair.

```
device(config)# crypto key client zeroize rsa
```

The following example shows how to delete DSA and RSA client key pairs from flash memory.

```
device(config)# crypto key client zeroize
```

crypto key generate

Generates the crypto key to enable SSH.

Syntax

crypto key generate [**dsa** | **rsa** [**modulus** *key-size*]]

Command Default

A crypto key is not generated and SSH is not enabled.

Parameters

dsa

Generates the DSA host key pair.

rsa

Generates the RSA host key pair.

modulus *key-size*

Specifies the modulus size of the RSA key pair, in bits. The valid values for the modulus size are from 1024 through 2048. The default value is 1024.

Modes

Global configuration mode

Usage Guidelines

The **dsa** keyword is optional. If you do not enter the dsa keyword, the crypto key generate command generates a DSA key pair by default.

To enable SSH, you generate a DSA or RSA host key on the device. The SSH server on the Brocade device uses this host DSA or RSA key, along with a dynamically generated server DSA or RSA key pair, to negotiate a session key and encryption method with the client trying to connect to it. While the SSH listener exists at all times, sessions cannot be started from clients until a host key is generated. After a host key is generated, clients can start sessions. When a host key is generated, it is saved to the flash memory of all management modules. The time to initially generate SSH keys varies depending on the configuration, and can be from a under a minute to several minutes.

To disable SSH, you delete all of the host keys from the device. When a host key is deleted, it is deleted from the flash memory of all management modules.

Examples

The following example shows how to generate the DSA host key pair.

```
device(config)# crypto key generate dsa
```

The following example shows how to generate the RSA key pair.

```
device(config)# crypto key generate rsa modulus 2014
```

crypto key zeroize

Deletes the crypto host key pair from the flash memory.

Syntax

crypto key zeroize [**dsa** | **rsa**]

Command Default

SSH is not enabled and the host key pair is saved in the flash memory.

Parameters

dsa

Deletes the DSA host key pair.

rsa

Deletes the RSA host key pair.

Modes

Global configuration mode

Usage Guidelines

When a host key is generated, it is saved to the flash memory of all management modules. The time to initially generate SSH keys varies depending on the configuration, and can be from a under a minute to several minutes. To disable SSH, you delete all of the host keys from the device. When a host key is deleted, it is deleted from the flash memory of all management modules.

Examples

The following example shows how to delete the DSA key pair.

```
device(config)# crypto key zeroize dsa
```

The following example shows how to delete the RSA key pair.

```
device(config)# crypto key zeroize rsa
```

The following example shows how to delete DSA and RSA key pairs from flash memory.

```
device(config)# crypto key zeroize
```

History

Release version	Command history
5.9.00	This command was modified. The **cr** option was removed.

crypto-ssl certificate

Generates or deletes a crypto SSL certificate.

Syntax

crypto-ssl certificate { **generate** | **zeroize** }

Parameters

generate

Generates an SSL certificate.

zeroize

Deletes the currently operative SSL certificate.

Modes

Global configuration mode

Usage Guidelines

To allow web management access through HTTPS, you must generate the SSL certificate in addition to enabling web management.

Examples

The following example shows how to generate a crypto SSL certificate.

```
device(config)# crypto-ssl certificate generate
```

The following example shows how to delete a crypto SSL certificate.

```
device(config)# crypto-ssl certificate zeroize
```

cycle-time

Sets a limit as to how many seconds users have to be authenticated by Web Authentication.

Syntax

cycle-time *seconds*

no cycle-time *seconds*

Command Default

The default is 600 seconds.

Parameters

seconds

Specifies the authentication cycle time. Valid values are from 0 through 3600 seconds. If the value is set to 0, then there is no limit.

Modes

Web Authentication configuration mode

Usage Guidelines

You can set a limit as to how many seconds users have to be authenticated by the Web Authentication by defining a cycle time. This time begins upon the first Login attempt by the user on the Login page. If the user has not been authenticated successfully when this time expires, the user must enter a valid URL again to display the Web Authentication Welcome page.

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

Examples

The following example sets the cycle time to 100 seconds.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# cycle-time 100
```

dampening

Sets dampening parameters for the route in BGP address-family mode.

Syntax

dampening { *half-life reuse suppress max-suppress-time* | **route-map** *route-map* }

no dampening

Parameters

half-life
: Number of minutes after which the route penalty becomes half its value. Range is from 1 through 45. Default is 15.

reuse
: Minimum penalty below which the route becomes usable again. Range is from 1 through 20000. Default is 750.

suppress
: Maximum penalty above which the route is suppressed by the device. Range is from 1 through 20000. Default is 2000.

max-suppress-time
: Maximum number of minutes a route can be suppressed by the device. Default is 40.

route-map
: Enables selection of dampening values established in a route map by means of the **route-map** command.

  route-map
  : Name of the configured route map.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

Use **dampening** without operands to set default values for all dampening parameters.

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 use the dampening values established in a route map, configure the route map first, and then enter the **route-map** command, followed by the name of the configured route map.

A full range of dampening values (*half-life*, *reuse*, *suppress*, *max-suppress-time*) can also be set by means of the **set as-path prepend** command.

Examples

This example enables default dampening as an IPv4 address-family function.

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

This example changes all the dampening values as an IPv6 address-family function.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# dampening 20 200 2500 40
```

This example applies the dampening half-life established in a route map, configures the route map using the **set dampening** command.

```
device# configure terminal
device(config)# route-map myroutemap permit 1
device(config-route-map myroutemap)# set dampening 20
```

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 seconds.

Parameters

number

Specifies the time interval for which the backup waits for the Hello message from the master. The time interval range is from 1 through 84 seconds.

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 1/1/1 to 1/1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# dead-interval 30
```

decnet-proto

Configures the DECnet protocol VLAN.

Syntax

decnet-proto [**name** *string*]

no decnet-proto [**name** *string*]

Command Default

The DECnet protocol VLAN is not configured.

Parameters

name *string*

Specifies the name of the DECnet protocol VLAN that you want to configure. The name can be up to 32 characters in length.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command removes the DECnet protocol VLAN.

Examples

The following example shows how to configure a DECnet protocol VLAN.

```
device(config)# vlan 2
device(config-vlan-2)# decnet-proto name Red
device(config-vlan-decnet-proto)# no dynamic
```

default-gateway

Configures the default gateway for a VLAN.

Syntax

default-gateway *ip-address metric*

no default-gateway *ip-address metric*

Command Default

The default gateway is not configured.

Parameters

ip-address

Specifies the IP address of the gateway router.

metric

Specifies the metric (cost) of the gateway. You can specify a value from 1 through 5. There is no default. The gateway with the lowest metric is used.

Modes

VLAN configuration mode

Usage Guidelines

You can configure up to five default gateways for the designated VLAN, and associate a metric with each one. The software uses the gateway with the lowest metric. The other gateways reside in the configuration but are not used. To use one of the other gateways, modify the configuration so that the gateway you want to use has the lowest metric. If more than one gateway has the lowest metric, the gateway that appears first in the running-config is used.

If you have already configured a default gateway globally using the **ip default-gateway** command and you do not configure a gateway in the VLAN, the software uses the globally configured gateway and gives the gateway a metric value of 1.

The **no** form of the command removes the gateway configuration for a VLAN.

Examples

The following example shows how to set the default gateway for a management VLAN. Because the 10.10.10.1 gateway has a lower metric, the software uses this gateway. The other gateway remains in the configuration, but is not used. You can use the other one by changing the metrics so that the 10.20.20.1 gateway has the lower metric.

```
device(config)# vlan 10
device(config-vlan-10)# default-gateway 10.10.10.1 1
device(config-vlan-10)# default-gateway 10.20.20.1 2
```

default-information-originate (BGP)

Configures the device to originate and advertise a default BGP4 or BGP4+ route.

Syntax

default-information-originate

no default-information-originate

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

Usage Guidelines

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

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.

Examples

This example originates and advertises a default BGP4 route.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# default-information-originate
```

This example originates and advertises a default BGP4 route in a nondefault VRF instance.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# default-information-originate
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

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 65535.

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 (BGP)

Changes the default metric used for redistribution.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 1.

Parameters

value

Metric value. Range is from 0 through 65535. The default metric value is 1.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This example changes the default metric used for redistribution to 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# default-metric 100
```

default-ports

Assigns ports (interfaces) other than the factory-assigned ports as the default stacking ports.

Syntax

default-ports *unit/slot/ port*

no default-ports

Command Default

The factory-assigned default stacking ports are the only default stacking ports on the device.

Parameters

unit
: Stack unit ID for the device on which the interface resides.

slot
: Stack unit slot or module on which the interface resides.

port
: Interface to be used as a default stacking port.

Modes

Stack unit configuration mode

Usage Guidelines

The **no** form of the command restores the factory-assigned default stacking ports. Any ports you previously assigned as the default stacking ports using the **default-ports** command are overwritten.

When you use the **default-ports** command, the factory-assigned default stacking ports are no longer the default stacking ports.

Only valid stacking ports can be assigned as default stacking ports. Valid ports vary depending on the type of FastIron device.

Tagged ports cannot be assigned as default stacking ports.

The number of ports you can assign as default stacking ports varies depending on the type of FastIron device. Some devices allow you to assign two ports as the default stacking ports, and some devices allow you to assign a single port as the default stacking port.

Examples

The following example assigns the stacking ports on Module 3 on the rear panel of an ICX 7750 as the default stacking ports.

```
device# configure terminal
device(config)# stack unit 1
device¡(config-unit-1)# default-ports 1/3/1 1/3/4
```

default-timers

Resets the GVRP Join, Leave, and Leaveall timers to the default values.

Syntax

default-timers

Command Default

The default value for the Join timer is 200 ms. The default value for the Leave timer is 600 ms. The default value for the Leaveall timer is 10,000 ms.

Modes

GVRP configuration mode

Usage Guidelines

You can use the **join-timer** command to change the values of these timers.

Examples

The following example shows how to reset the timers to the default values.

```
device(config)# gvrp-enable
device(config-gvrp)# default-timers
```

default-vlan-id

Changes the default VLAN ID.

Syntax

default-vlan-id *vlan-id*

no default-vlan-id *vlan-id*

Command Default

The default VLAN ID is 1.

Parameters

vlan-id

Specifies the VLAN ID that you want to configure as the default. Valid VLAN ID values are from 1 through 4095.

Modes

Global configuration mode

Usage Guidelines

You must specify a valid VLAN ID that is not already in use. For example, if you have already defined VLAN 10, you cannot use "10" as the new VLAN ID for the default VLAN.

NOTE
This command does not change the properties of the default VLAN. Changing the name allows you to use the VLAN ID "1" as a configurable VLAN.

The **no** form of the command resets the VLAN ID to the default.

Examples

The following example shows how to change the default VLAN ID.

```
device(config)# default-vlan-id 4095
```

delay-notifications

Configures the delay time for notifying the Layer 3 protocols of the VE down event.

Syntax

delay-notifications *value*

no delay-notifications *value*

Command Default

The delay time is not configured.

Parameters

value

The time to delay the notification of the VE down event. The value can range from 1 through 60 seconds.

Modes

VE interface configuration mode

Usage Guidelines

When all the ports in the VLAN go into the non-forwarding state, the device waits for the configured time before notifying the Layer 3 protocols of the VE down event. Once the timer expires, if the ports remain in the non-forwarding state, the device notifies the Layer 3 protocols of the VE down event.

If any of the ports comes into the forwarding state before the timer expires, the device cancels the existing timer for the VE down event.

The **no** form of the command removes the configured delay time.

Examples

The following example shows configuring the delay time on interface 50 to 20 seconds.

```
device(config)#  interface ve 50
device(config-vif-50)# delay-notifications 20
```

History

Release version	Command history
08.0.30b	This command was introduced.

delete-all

Deletes all user records from a local user database.

Syntax

delete-all

Modes

Local user database configuration mode

Examples

The following example deletes all user records from the local user database "localdb1".

```
device(config)# local-userdb localdb1
device(config-localuserdb-localdb1)# delete-all
```

deploy

Deploys the LAG.

Syntax

deploy [**passive**]

no deploy [**passive**]

Command Default

The LAG is not deployed.

Parameters

passive

Configures Link Aggregation Control Protocol (LACP) as passive. This option is applicable only to dynamic LAGs and LACP is active by default.

Modes

LAG configuration mode

Usage Guidelines

A LAG must be created before being deployed. After configuring a LAG, you must explicitly enable it before it begins aggregating traffic. This task is accomplished by executing the **deploy** command within the LAG configuration. After the **deploy** command runs, the LAG is in the aggregating mode.

To deploy a LAG, at least one port must be in the LAG and the primary port must be specified for non-keep-alive LAGs. After a non-keep-alive LAG is deployed, a LAG is formed. If there is only one port in the LAG, a single port LAG is formed. For a dynamic LAG, LACP is started for each LAG port. For a keep-alive LAG, no LAG is formed and LACP is started on the LAG port.

When activating LACP, LACP is activated as active if the **passive** keyword is not specified. If you need to configure LACP as passive, use the **passive** keyword. Once the **deploy** command is issued, all LAG ports will behave like a single port. For dynamic LAGs, LACP is activated on all of the LAG ports.

The **no** form of the command undeploys the LAG. Once the LAG is undeployed, all the secondary ports are disabled automatically and there will be no changes to the primary port. Also, for dynamic LAGs, LACP is deactivated on all ports.

Examples

The following example shows how to deploy a LAG.

```
device(config)# lag blue static
device(config-lag-blue)# deploy
```

The following example shows how to deploy a dynamic LAG as passive.

```
device(config)# lag test2 dynamic
device(config-lag-test2)# deploy passive
```

dhcp-default-router

Specifies the IP addresses of the default routers for a client.

Syntax

dhcp-default-router *address*

Parameters

address

Specifies the IP address of the default router.

Modes

DHCP server pool configuration mode

Examples

The following example specifies the IP address of the default router for a client.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# dhcp-default-router 10.2.1.143
```

dhcp-gateway-list

Configures a gateway list when DHCP Assist is enabled on a Layer 2 switch.

Syntax

dhcp-gateway-list *num ip-address*

Parameters

num

Specifies the number of the gateway list.

ip-address

Specifies the gateway IP address.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

Up to eight addresses can be defined for each gateway list in support of ports that are multi-homed. When multiple IP addresses are configured for a gateway list, the Layer 2 switch inserts the addresses into the discovery packet in a round-robin fashion. Up to 32 gateway lists can be defined for each Layer 2 switch.

Examples

The following commands configure a gateway list.

```
device(config)# dhcp-gateway-list 1 10.95.5.1
device(config)# dhcp-gateway-list 2 10.95.6.1
device(config)# dhcp-gateway-list 3 10.95.1.1 10.95.5.1
device(config)# interface ethernet 2
device(config-if-e1000-2)# dhcp-gateway-list 1
device(config-if-e1000-2)# interface ethernet 8
device(config-if-e1000-8)# dhcp-gateway-list 3
device(config-if-e1000-8)# interface ethernet 14
device(config-if-e1000-14)# dhcp-gateway-list 2
```

dhcp snooping client-learning disable

Disables DHCP client learning on an individual port.

Syntax

dhcp snooping client-learning disable

no dhcp snooping client-learning disable

Modes

Interface configuration mode.

Usage Guidelines

Use the no form of the command to re-enable DHCP client learning on a port once it has been disabled.

Examples

The following example disables DHCP client learning on an individual port.

```
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# dhcp snooping client-learning disable
```

History

Release version	Command history
	This command was introduced.
	This command was modified to...

dhcp snooping relay information option subscriber-id

Configures a unique subscriber ID per port.

Syntax

dhcp snooping relay information option subscriber-id *ASCII string*

no dhcp snooping relay information option subscriber-id *ASCII string*

Parameters

ASCII string

Specifies the ASCII string. The string can be up to 50 alphanumeric characters in length.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables SID processing once it is enabled.

Use the **show interfaces ethernet** command to view the subscriber ID configured on a port.

Examples

The following example enables a unique subscriber ID per port.

```
device(config)# ip dhcp snooping vlan 1
device(config)# interface ethernet 1/1/4
device(config-if-e1000-1/1/4)# dhcp snooping relay information option subscriber-id Brcd01
```

dhcp snooping trust

Enables trust on a port connected to a DHCP server.

Syntax

dhcp snooping trust

no dhcp snooping trust

Command Default

The default trust setting for a port is untrusted.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables the trust setting.

Examples

The following example sets the trust setting of port 1/1/1 to trusted.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# dhcp snooping trust
```

dhcp6 snooping trust

Enables trust on a port connected to a DHCPv6 server.

Syntax

dhcp6 snooping trust

no dhcp6 snooping trust

Command Default

The default trust setting for a port is untrusted

Modes

Interface configuration mode.

Usage Guidelines

The no form of the command disables trust on the port.

Examples

The following example enables trust on a port connected to a DHCPv6 server.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# dhcp6 snooping trust
```

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-aging

Disables aging of MAC sessions at the global level.

Syntax

disable-aging [**permitted-mac-only** | **denied-mac-only**]

no disable-aging [**permitted-mac-only** | **denied-mac-only**]

Command Default

Aging of MAC sessions is not disabled.

Parameters

permitted-mac-only

Prevents permitted (authenticated and restricted) sessions from being aged out and ages denied sessions.

denied-mac-only

Prevents denied sessions from being aged out, but ages out permitted sessions.

Modes

Authentication mode

Usage Guidelines

The **no** form of the command does not disable aging.

Use this command to disable the aging of MAC sessions. Use the **disable-aging** command in the authentication mode and the **authentication disable-aging** command at the interface level. The command entered at the interface level overrides the command entered at the authentication level.

Examples

The example disables aging for permitted MAC addresses.

```
device(config)# authentication
device(config-authen)# disable-aging permitted-mac-only
```

History

Release version	Command history
08.0.20	This command was introduced.

disable (LAG)

Disables the individual ports within a LAG.

Syntax

disable port-name *name*

disable ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

LAG ports are not enabled.

Parameters

port-name *name*
Disables a named port within a LAG.

ethernet *stackid/slot/port*
Disables the Ethernet port within a LAG.

to *stackid/slot/port*
Disables a range of ports within a LAG.

Modes

LAG configuration mode

Usage Guidelines

To disable a port belonging to a keep-alive LAG, you must configure the **enable** command from the interface configuration mode.

NOTE
You cannot disable a LAG Ethernet port unless it is deployed.

Examples

The following example shows how to disable a port within a LAG.

```
device(config)# lag blue static
device(config-lag-blue)# deploy
device(config-lag-blue)# disable ethernet 1/3/1
```

The following example shows how to disable a port within a keep-alive LAG.

```
device(config)# lag test keep-alive
device(config-lag-test)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# disable
```

disable (NTP)

Disables the NTP server and client mode.

Syntax

disable [**serve**]

no disable serve

Parameters

serve

Disables serving time to clients.

Command Default

NTP is enabled using the **ntp** command.

Modes

NTP configuration mode

Usage Guidelines

To enable the client mode, use the **no disable** command. To enable the client and server mode, use the **no disable serve** command. The **no disable** command enables both client and server. If the client is already enabled and server is disabled at that time then**no disable server** enables the server.

If the **serve** keyword is specified, then NTP will not serve the time to downstream devices. The **serve** keyword disables the NTP server mode functionalities. If the **serve** keyword is not specified, then both NTP client mode and NTP server mode is disabled.

NOTE
The **disable** command disables the NTP server and client mode; it does not remove the NTP configuration.

The **no** form of the command enables the NTP client and server mode.

Examples

The following example shows how to disable the NTP server.

```
device(config)# ntp
device(config-ntp)# disable serve
```

disable (Port)

Disables a port.

Syntax

disable

Command Default

A port is enabled (active).

Modes

Interface configuration mode

Usage Guidelines

A port can be deactivated (disabled) or activated (enabled) using the **enable** command by selecting the appropriate status.

Examples

The following example disables or inactivate a port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# disable
```

disable (VSRP)

Disables the VSRP VRID for a port-based VLAN.

Syntax

disable

Command Default

The VSRP VRID is disabled by default.

Modes

VSRP VRID configuration mode

Examples

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

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

disable authentication md5

Disables the MD5 authentication scheme for Network Time Protocol (NTP).

Syntax

disable authentication md5

no disable authentication md5

Command Default

If JITC is enabled, the MD5 authentication scheme is disabled. In the standard mode, the MD5 authentication scheme is enabled.

Modes

Global configuration mode

Usage Guidelines

In the standard mode, both SHA1 and MD5 authentication schemes are supported. If JITC is enabled, The MD5 authentication for Network Time Protocol (NTP) is disabled by default and the **disable authentication md5** command can be seen in the running configuration. In the JITC mode, only the SHA1 option is available. The SHA1 authentication scheme must be enabled manually to define the authentication key for NTP using the **authentication-key key-id** command.

The **no** form of the command enables the MD5 authentication scheme.

Examples

The following example disables the MD5 authentication scheme.

```
device(config)# disable authentication md5
```

History

Release version	Command history
08.0.20a	This command was introduced.

distance (BGP)

Changes the default administrative distances for EBGP, IBGP, and local BGP.

Syntax

distance *external-distance internal-distance local-distance*

no distance

Parameters

external-distance
EBGP distance. Range is from 1 through 255.

internal-distance
IBGP distance. Range is from 1 through 255.

local-distance
Local BGP4 and BGP4+ distance. Range is from 1 through 255.

Modes

BGP configuration mode

Usage Guidelines

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-router)# distance 100 150 200
```

dlb-internal-trunk-hash

Changes the hashing method for inter-packet-processor (inter-pp) HiGig links that are used to connect master and slave units in ICX 7450-48 devices.

Syntax

dlb-internal-trunk-hash { **inactivity-mode** | **spray-mode** }

no dlb-internal-trunk-hash { **inactivity-mode** | **spray-mode** }

Command Default

The hashing method is inactivity mode.

Parameters

inactivity-mode

Specifies that the flow is set by the inactivity of traffic loading.

spray-mode

Specifies that the flow is set to receive new member assignments for every packet arrival in accordance with the traffic loading of each aggregate member.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default hashing method.

NOTE
This command is supported only on ICX 7450-48 devices that have master and slave units.

Dynamic load balancing (DLB) enhances hash-based load balancing by taking into account the traffic loading in the network. The inter-pp HiGig links in ICX7450-48 devices use hash-based load balancing to distribute traffic evenly. You can configure the **dlb-internal-trunk-hash** command to change the hashing method.

Examples

The following example globally enables spray mode as the inter-pp links hashing method.

```
ICX7450-48P Router(config)#dlb-internal-trunk-hash  spray-mode
```

History

Release version	Command history
08.0.20	This command was introduced.

dns-filter

Defines Domain Name System (DNS) filters that will restrict DNS queries from unauthenticated hosts to be forwarded explicitly to defined servers.

Syntax

dns-filter *filter-id ip-address wildcard-bits*

no dns-filter *filter-id ip-address wildcard-bits*

Command Default

DNS filters are not defined.

Parameters

filter-id
: Defines the number to identify a DNS filter. The valid values are from 1 through 4.

ip-address
: Specifies the IP address (A.B.C.D) or IP address along with the prefix length (A.B.C.D/n) of unauthenticated hosts.

wildcard-bits
: Specifies a wildcard for the filter. The wildcard is in dotted-decimal notation (IP address format).

Modes

Web Authentication configuration mode

Usage Guidelines

Many of the Web Authentication solutions allow DNS queries to be forwarded from unauthenticated hosts. To eliminate the threat of forwarding DNS queries from unauthenticated hosts to unknown or untrusted servers (also known as domain-casting), you can restrict DNS queries from unauthenticated hosts to be forwarded explicitly to defined servers by defining DNS filters. Any DNS query from an unauthenticated host to a server that is not defined in a DNS filter is dropped. Only DNS queries from unauthenticated hosts are affected by DNS filters; authenticated hosts are not. If the DNS filters are not defined, then any DNS queries can be made to any server.

The wildcard is in dotted-decimal notation (IP address format). It is a four-part value, where each part is 8 bits (one byte) separated by dots, and each bit is a one or a zero. Each part is a number ranging from 0 to 255, for example 0.0.0.255. Zeros in the mask mean the packet source address must match the IP address. Ones mean any value matches. For example, the IP address and subnet-mask values 10.157.22.26 0.0.0.255 mean that all hosts in the Class C subnet 10.157.22.x match the policy.

The **no** form of the command removes the defined DNS filters.

Examples

The following example defines a DNS filter.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# dns-filter 2 192.168.10.1/24 0.0.0.255
```

domain-name

Configures the domain name for the DHCP client.

Syntax

domain-name *domain-name*

Parameters

domain-name

Specifies the name of the domain.

Modes

DHCP server pool configuration mode

Examples

The following example specifies the domain name for the DHCP client.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# domain-name sierra
```

dot1x auth-fail-action restricted-vlan

Configures an individual port to place the client port in a specific restricted VLAN when dot1x port authentication fails.

Syntax

dot1x auth-fail-action restricted-vlan *vlan-id*

no dot1x auth-fail-action restricted-vlan *vlan-id*

Parameters

vlan-id

Specifies the VLAN to be used as the restricted VLAN.

Modes

Interface configuration mode

Usage Guidelines

You cannot configure the authentication failure action globally and per-port at the same time.

The **no** form of the command removes the authentication failure action on the individual port.

Examples

The following example configures the placing of the client port in restricted VLAN 300 when authentication fails.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# dot1x auth-fail-action restricted-vlan 300
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

dot1x auth-filter

Applies the specified filter on the interface and the MAC addresses defined in the filter (MAC filter) do not have to go through authentication.

Syntax

dot1x auth-filter *filter-id vlan-id*

no dot1x auth-filter *filter-id vlan-id*

Command Default

There are no filters applied on the interface.

Parameters

filter-id

Specifies the filter ID to be applied on the interface.

vlan-id

Specifies the VLAN ID.

Modes

Interface configuration mode

Usage Guidelines

A client can be authenticated in an untagged VLAN or tagged VLAN using the MAC address filter for 802.1X authentication.

If auth-filter has tagged VLAN configuration, the clients are authenticated in auth-default VLAN and tagged VLAN provided in auth-filter. The clients authorized in auth-default VLAN allow both untagged and tagged traffic.

The following rules apply when using the **dot1x auth-filter** command:

- The maximum number of filters that can be bound to a port is limited by the mac-filter-port default or a configured value.
- The filters must be applied as a group. For example, if you want to apply four filters to an interface, they must all appear on the same command line.
- You cannot add or remove individual filters in the group. To add or remove a filter on an interface, apply the filter group again containing all the filters you want to apply to the port.
- If you apply a filter group to a port that already has a filter group applied, the older filter group is replaced by the new filter group.
- If you add filters to or modify the 802.1X authentication filter, the system clears all 802.1X sessions on the port. Consequently, all users that are logged in will need to be re-authenticated.

The **no** form of the command disable the dot1x auth-filter functionality. If the VLAN is not specified, the auth-default-vlan is used.

Examples

The following example applies the dot1x filter on a specific VLAN.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# dot1x auth-filter 1 2
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x auth-timeout-action

Configures the RADIUS timeout behavior to bypass 802.1X(dot1x) authentication and permit or deny user access to the network.

Syntax

dot1x auth-timeout-action { **failure** | **success** }

no dot1x auth-timeout-action { **failure** | **success** }

Command Default

The device resets the authentication process and retries to authenticate the user.

Parameters

failure

Bypasses the authentication process and blocks user access to the network unless **dot1x auth-fail-action restricted-vlan** command is configured, in which case, the user is placed into a VLAN with restricted or limited access.

success

Bypasses the authentication process and permits user access to the network.

Modes

Interface configuration mode

Usage Guidelines

If **dot1x auth-fail-action restricted-vlan** is configured along with **dot1x auth-timeout-action failure**, the user will be placed into a VLAN with restricted or limited access.

The **no** form of the command resets the RADIUS timeout behavior to **retry**.

Examples

The following example configures the RADIUS timeout behavior to bypass 802.1X authentication and block user access to the network.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# dot1x auth-timeout-action failure
```

The following example configures the RADIUS timeout behavior to bypass dot1x authentication and permit user access to the network.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# dot1x auth-timeout-action success
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

dot1x disable-filter-strict-security

Disables strict security mode for 802.1X dynamic filter assignment on a specific interface.

Syntax

dot1x disable-filter-strict-security

no dot1x disable-filter-strict-security

Command Default

Strict security mode is enabled for all 802.1X-enabled interfaces.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command re-enables strict security mode for 802.1X dynamic filter assignment on the interface.

Examples

The following example disables strict security mode for 802.1X dynamic filter assignment on a specific interface.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# dot1x disable-filter-strict-security
```

The following example re-enables strict security mode for 802.1X dynamic filter assignment on a specific interface.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# no dot1x disable-filter-strict-security
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

dot1x enable

Enables 802.1X authentication.

Syntax

dot1x enable

dot1x enable all

dot1x enable ethernet *stackid/slot/port*

no dot1x enable [**all** | **ethernet** *stackid/slot/port*]

Command Default

802.1X authentication is not enabled.

Parameters

all

Enables 802.1X authentication on all interfaces.

ethernet *stackid/slot/port*

Enables 802.1X authentication on the specified interface.

Modes

Authentication configuration mode

Usage Guidelines

The **dot1x enable** command without any options initializes 802.1X authentication feature globally. The **dot1x enable** command with the **all** or **ethernet** options, enables 802.1X authentication on all or a specific interface respectively. After initializing 802.1X authentication feature using the **dot1x enable** command, you must enable 802.1X authentication on all or a specific interface.

Port control must be configured to activate authentication on an 802.1X-enabled interface using the **dot1x port-control** command from the interface configuration mode.

The **no** form of the command disables 802.1X authentication.

Examples

The following example enables 802.1X authentication on all interfaces.

```
device(config)# authentication
device(config-authen)# dot1x enable
device(config-authen)# dot1x enable all
```

The following example shows enabling 802.1X authentication on ethernet interface 1/1/1.

```
device(config)# authentication
device(config-authen)# dot1x enable
device(config-authen)# dot1x enable ethernet 1/1/1
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x guest-vlan

Specifies the VLAN into which the port should be placed when the client's response to the dot1x requests for authentication times out.

Syntax

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan *vlan-id*

Command Default

The guest VLAN ID is not specified.

Parameters

vlan-id

Specifies the VLAN ID of the guest VLAN.

Modes

dot1x configuration mode.

Usage Guidelines

The **no** form of this command disables the functionality.

Use this command when the client does not support the 802.1X authentication, so that the client can access default privileges.

If there is no response from dot1x client for EAP-packets and if guest VLAN is not configured, authentication is considered as failed and the configured failure action is performed.

Examples

The following example specifies the guest VLAN.

```
device(config)# authentication
device(config-authen)# dot1x guest-vlan 7
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x initialize

Initializes 802.1X authentication on a port.

Syntax

dot1x initialize ethernet *slot/port*

Parameters

ethernet *slot/port*

Specifies the details of the interface on which 802.1x authentication is to be initialized.

Modes

Privileged EXEC mode

Examples

The following example initializes dot1x authentication on a port.

```
device# dot1x initialize ethernet 3/1
```

dot1x max-reauth-req

Configure the maximum number of times (attempts) EAP-request/identity frames are sent for reauthentication after the first authentication attempt.

Syntax

dot1x max-reauth-req *count*

no dot1x max-reauth-req *count*

Command Default

The device sends the EAP-request/identity frames for reauthentication twice.

Parameters

count

Specifies the number of EAP frame re-transmissions. This is a number from 1 through 10. The default is 2.

Modes

Authentication configuration mode

Usage Guidelines

The **no** form of this command will disable this functionality.

The Brocade device retransmits the EAP-request/identity frame a maximum of two times. If no EAP response/identity frame is received from the client after two EAP-request/identity frame re-transmissions (or the amount of time specified with the max-reauth-req command), the device restarts the authentication process with the client.

You can optionally change the number of times the Brocade device should retransmit the EAP request/identity frame.

Examples

The following example configures the device to retransmit an EAP-request/identity frame to a client a maximum of three times.

```
device(config)# authentication
device(config-authen)# dot1x max-reauth-req 3
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x max-req

Configures the maximum number of times EAP request/challenge frames are retransmitted when EAP response/identity frame is not received from the client.

Syntax

dot1x max-req *count*

no dot1x max-req *count*

Command Default

The device retransmits the EAP-request/challenge twice.

Parameters

count

Specifies the number of EAP frame re-transmissions. This is a number from 1 through 10. The default is 2.

Modes

Authentication configuration mode

Usage Guidelines

The **no** form of this command will disable this functionality.

Examples

The following example configures the device to retransmit an EAP-request/challenge frame to a client a maximum of three times.

```
device(config)# authentication
device(config-authen)# dot1x max-req 3
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x-mka-enable

Enables MACsec Key Agreement (MKA) capabilities on a licensed device and enters dot1x-mka configuration mode.

Syntax

dot1x-mka-enable

no dot1x-mka-enable

Command Default

No MACsec capability is available.

Modes

Global configuration

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

The **no** form of this command disables the MKA and MACsec functionality on all ports. This may require the already authenticated hosts to re-authenticate.

Use the **dot1x-mka-enable** command to enable MACsec on an already licensed device. Commands may be visible, but they do not work on a non-licensed device.

Examples

The following example enables MACsec capabilities on the device.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)#
```

History

Release version	Command history
08.0.20	This command was introduced.

Related Commands

enable-mka, mka-cfg-group

dot1x port-control

Configures the port control type to activate authentication on an 802.1X-enabled interface.

Syntax

dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

no dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

Command Default

All controlled ports on the device are in the authorized state, allowing all traffic.

Parameters

auto

Places the controlled port in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized. This activates authentication on an 802.1X-enabled interface. The controlled port remains in the authorized state until the Client logs off.

force-authorized

Places the controlled port unconditionally in the authorized state, allowing all traffic to pass between the client and the authenticator. This is the default state for ports on the Brocade device.

force-unauthorized

Places the controlled port unconditionally in the unauthorized state, denying any traffic to pass between the client and the authenticator.

Modes

Interface configuration mode

Usage Guidelines

Before activating the authentication using the **dot1x port-control** auto command on an untagged port, you must remove configured static ACL, if any, from the port.

You cannot enable 802.1X authentication on ports that have any of the following features enabled:

- Link aggregation
- Metro Ring Protocol (MRP)
- Mirror port
- LAG port
- DHCP snooping
- ARP inspection

The **no** form of the command resets the port control type to the default state (force-authorized) allowing all traffic to pass between the client and the authenticator.

Examples

The following example configures the interface to place its controlled port in the authorized state when a client is authenticated by an authentication server.

```
device(config)# interface ethernet 3/1/1
device(config-if-e100-3/1/1)# dot1x port-control auto
```

The following example configures the interface to place the controlled port unconditionally in the authorized state.

```
device(config)# interface ethernet 3/1/1
device(config-if-e100-3/1/1)# dot1x port-control force-authorized
```

The following example configures the interface to place the controlled port unconditionally in the unauthorized state.

```
device(config)# interface ethernet 3/1/1
device(config-if-e100-3/1/1)# dot1x port-control force-unauthorized
```

dot1x re-authenticate

Re-authenticates the clients connected to a specific port manually.

Syntax

dot1x re-authenticate ethernet *slot/port*

Parameters

ethernet *slot/port*

Specifies the details of the interface to which the clients are connected.

Modes

Privileged EXEC mode

Usage Guidelines

When periodic re-authentication is enabled, by default the Brocade device re-authenticates clients connected to an 802.1X-enabled interface every 3,600 seconds (or the time specified by the **timeout re-authperiod** command). The **dot1x re-authenticate** command allows you to manually re-authenticate clients connected to a specific port.

Examples

The following example re-authenticates the clients connected to a specific port.

```
device# dot1x re-authenticate ethernet 3/1
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

dot1x re-auth-timeout-success

Configures RADIUS timeout behavior to bypass MAC authentication and permit user access to the network.

Syntax

dot1x re-auth-timeout-success *seconds*

no dot1x re-auth-timeout-success *seconds*

Command Default

The authentication is considered as failed after timeout.

Parameters

seconds

Specifies the number of seconds the device will wait to bypass MAC authentication and permit user access to the network after a timeout.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command resets the RADIUS timeout behavior to consider the authentication as failed.

Examples

The following example configures RADIUS timeout behavior to bypass MAC authentication and permit user access to the network.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# dot1x re-auth-timeout-success 60
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

dot1x timeout

Configures the timeout parameters that determine the time interval for client reauthentication and EAP retransmissions.

Syntax

dot1x timeout {**quiet-period** *seconds*| **supplicant** *seconds* | **tx-period** *seconds* }

no dot1x timeout {**quiet-period** *seconds*| **supplicant** *seconds* | **tx-period** *seconds* }

Command Default

The timeout parameters are not applied to the device.

Parameters

quiet-period *seconds*

Specifies the time, in seconds, the device waits before trying to re-authenticate the client. The quiet period can be from 1 through 4294967295 seconds. The default is 60 seconds. If the Brocade device is unable to authenticate the client, the Brocade device waits a specified amount of time before trying again. The amount of time the Brocade device waits is specified with the quiet period parameter.

supplicant *seconds*

By default, when the Brocade device relays an EAP-Request frame from the RADIUS server to the client, it expects to receive a response from the client within 30 seconds. You can optionally specify the wait interval using the **supplicant** *seconds* parameters. The value is 1 through 4294967295.

tx-period *seconds*

Specifies the EAP request retransmission interval, in seconds, with the client. By default, if the Brocade device does not receive an EAP-response/identity frame from a client, the device waits 30 seconds, then retransmits the EAP-request/identity frame. You can optionally change the amount of time the Brocade device waits before re-transmitting the EAP-request/identity frame to the client. If the client does not send back an EAP-response/identity frame within 60 seconds, the device will transmit another EAP-request/identity frame. The tx-period is a value from 1 through 4294967295. The default is 30 seconds.

Modes

Authentication configuration mode

Usage Guidelines

The **no** form of the command disables dot1x timeout.

Examples

The following example specifies the quiet period as 30 seconds.

```
device(config)# authentication
device(config-authen)# dot1x enable
device(config-authen)# dot1x timeout quiet-period 30
```

History

Release version	Command history
08.0.20	This command was introduced.

dot1x-enable

Enables 802.1X authentication and enters the dot1x configuration level.

Syntax

dot1x-enable

no dot1x-enable

Command Default

dot1x authentication is disabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables 802.1X authentication.

Examples

The following example enables dot1x authentication and enters the 802.1X configuration level.

```
device(config)# dot1x-enable
device(config-dot1x)#
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

dual-mode

Configures a tagged port to accept and transmit both tagged and untagged traffic at the same time.

Syntax

dual-mode [*vlan-id*]

no dual-mode [*vlan-id*]

Command Default

Dual mode is disabled.

Parameters

vlan-id

Specifies the default VLAN ID for the dual-mode port.

Modes

Interface configuration mode

Usage Guidelines

If you do not specify a VLAN ID, the port default VLAN is set to 1. The port transmits untagged traffic on the default VLAN.

A dual-mode port accepts and transmits frames belonging to VLANs configured for the port, as well as frames belonging to the default VLAN (that is, untagged traffic). You can configure a dual-mode port to transmit traffic for a specified VLAN (other than the default VLAN) as untagged, while transmitting traffic for other VLANs as tagged. Only tagged ports can be configured as dual-mode ports.

In a LAG, either all of the ports must be in dual-mode, or none of them can be.

You can configure multiple ports to be in dual mode.

NOTE
An error message is displayed while attempting to configure an existing dual mode on a port range.

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

Examples

The following example shows how to configure dual mode, allowing traffic for VLAN 20 and untagged traffic to go through port 2/11 at the same time.

```
device(config)# vlan 20
device(config-vlan-20)# tagged ethernet 2/11
device(config-vlan-20)# tagged ethernet 2/9
device(config-vlan-20)# interface ethernet 2/11
device(config-if-e1000-2/11)# dual-mode
device(config-if-e1000-2/11)# exit
```

The following example shows configuring a dual-mode port to transmit traffic for a specified VLAN (other than the default VLAN) as untagged, while transmitting traffic for other VLANs as tagged. Tagged port 2/11 is added to VLANs 10 and 20, and then designated a dual-mode port whose specified default VLAN is 10.

```
device(config)# vlan 10 by port
device(config-vlan-10)# untagged ethernet 2/10
device(config-vlan-10)# tagged ethernet 2/11
device(config-vlan-10)# exit
device(config)# vlan 20 by port
device(config-vlan-20)# tagged ethernet 2/9
device(config-vlan-20)# tagged ethernet 2/11
device(config-vlan-20)# exit
device(config)# interface ethernet 2/11
device(config-if-e1000-2/11)# dual-mode 10
device(config-if-e1000-2/11)# exit
```

The following example shows how to configure multiple ports.

```
device# interface ethernet 1/1/6 to 1/1/9
device (config-mif-1/1/6-1/1/9)# dual-mode
```

dynamic

Configures dynamic ports.

Syntax

dynamic

no dynamic

Command Default

Ports are static.

Modes

Protocol VLAN configuration mode

Usage Guidelines

Dynamic ports within any protocol VLAN age out after 10 minutes if no member protocol traffic is received on a port within the VLAN. Once you dynamically add a port to a protocol VLAN, you cannot configure routing parameters on the port. You cannot dynamically add a port to a protocol VLAN if the port has any routing configuration parameters.

NOTE
Dynamic addition and removal of ports is not applicable for an AppleTalk protocol VLAN. You cannot route to or from protocol VLANs with dynamically added ports. In the switch image, all the ports are dynamic ports by default.

The **no** form of the command removes the dynamic setting.

Examples

The following example shows the IP protocol VLAN configured with dynamic ports.

```
device(config)# vlan 10
device(config-vlan-10)# ip-proto name IP_Prot_VLAN
device(config-vlan-ip-proto)# dynamic
```

The following example shows configuring port-based VLAN 10, and then configuring an IP subnet VLAN within the port-based VLAN with dynamic ports.

```
device(config)# vlan 10 name IP_VLAN by port
device(config-vlan-10)# untagged ethernet 1/1/1 to 1/1/6
added untagged port ethernet 1/1/1 to 1/1/6 to port-vlan 10.
device(config-vlan-10)# ip-subnet 10.1.1.0/24 name Mktg-LAN
device(config-vlan-ip-subnet)# dynamic
```

The following example shows configuring port-based VLAN 20, and then configuring an IPX network VLAN within the port-based VLAN with dynamic ports. These commands create a port-based VLAN on chassis ports 1/2/1 through 1/2/6 named "Eng-LAN", configure an IPX network VLAN within the port-based VLAN, and then add ports from the port-based VLAN dynamically.

```
device(config)# vlan 20 name IPX_VLAN by port
device(config-vlan-10)# untagged ethernet 1/2/1 to 1/2/6
added untagged port ethernet 1/2/1 to 1/2/6 to port-vlan 20.
device(config-vlan-10)# ipx-network abcd ethernet_ii name Eng-LAN
device(config-vlan-ipx-network)# dynamic
```

eee

Enables Energy Efficient Ethernet (EEE) globally, per port or on a range of ports.

Syntax

eee

no eee

Command Default

Energy Efficient Ethernet is not enabled.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of the command disables Energy Efficient Ethernet.

Examples

The following example enables Energy Efficient Ethernet globally.

```
device(config)# eee
EEE Feature Enabled
```

The following example enables Energy Efficient Ethernet on multiple ports.

```
device(config)# interface ethernet 1/1/1 to 1/1/12
device(config-mif-1/1/1-1/1/12)# eee
EEE Feature Enabled
EEE Feature Enabled on port 1/1/1
EEE Feature Enabled on port 1/1/2
EEE Feature Enabled on port 1/1/3
EEE Feature Enabled on port 1/1/4
EEE Feature Enabled on port 1/1/5
EEE Feature Enabled on port 1/1/6
EEE Feature Enabled on port 1/1/7
EEE Feature Enabled on port 1/1/8
EEE Feature Enabled on port 1/1/9
EEE Feature Enabled on port 1/1/10
EEE Feature Enabled on port 1/1/11
EEE Feature Enabled on port 1/1/12
```

The following example enables Energy Efficient Ethernet per port.

```
device(config)# interface ethernet e1000-1/1/1
device(config-if-e1000-1/1/1)# eee
EEE Feature Enabled EEE on port 1/1/1
```

History

Release version	Command history
08.0.30	This command was introduced.

egress-buffer-profile

Attaches a user-configured egress buffer profile to one or more ports.

Syntax

egress-buffer-profile *profile-name*

no egress-buffer-profile *profile-name*

Command Default

If a port is not attached to a user-configured egress buffer profile, it uses the default egress buffer profile.

Parameters

profile-name

Specifies the name of the egress buffer profile to be attached to the port.

Modes

Interface mode

Multiple-interface mode

Usage Guidelines

The **no** form of this command removes a user-configured egress buffer profile from the port and the port uses the default egress buffer profile.

You must configure an egress buffer profile before you can attach it to a port.

Only one egress buffer profile at a time can be attached to any port. You can attach an egress buffer profile to more than one port.

Examples

The following example attaches an egress buffer profile named egress1 to a port:

```
Device(config-if-e10000-1/1/1)# egress-buffer-profile egress1
```

The following example attaches an egress buffer profile named egress2 to multiple ports:

```
Device(config-mif-1/1/2-1/1/16)# egress-buffer-profile egress2
```

The following example removes an egress buffer profile named egress2 from multiple ports:

```
Device(config-mif-1/1/2-1/1/16)# no egress-buffer-profile egress2
```

History

Release version	Command history
8.0.10	This command was introduced.

enable (802.1X authentication)

Enables 802.1X authentication on all interfaces at once, on individual interfaces, or on a range of interfaces.

Syntax

enable { **all** | **ethernet** *slot/port* [[**to** *slot/port*] [**ethernet** *slot/port*]...] }

no enable { **all** | **ethernet** *slot/port* [[**to** *slot/port*] [**ethernet** *slot/port*]...] }

Command Default

dot1x authentication is disabled.

Parameters

all

Specifies to enable 802.1X authentication on all interfaces on the device.

ethernet *slot/port*

Specifies a specific interface on which 802.1X authentication must be enabled.

to *slot/port*

Specifies the range of interfaces on which 802.1X authentication must be enabled.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command disables 802.1X authentication.

Examples

The following example enables 802.1X authentication on all interfaces on the device.

```
device(config)# dot1x-enable
device (config-dot1x)# enable all
```

The following example enables 802.1X authentication on interface 3/11.

```
device(config)# dot1x-enable
device (config-dot1x)# enable ethernet 3/11
```

The following example enables 802.1X authentication on a range of interfaces.

```
device(config)# dot1x-enable
device (config-dot1x)# enable ethernet 3/11 to 3/16
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, Brocade ICX 7750, and Brocade ICX 7450.

enable aaa console

Enables AAA support for commands entered at the console.

Syntax

enable aaa console

no enable aaa console

Command Default

Command authorization and command accounting for console commands are not enabled.

Modes

Global configuration mode

Usage Guidelines

The Brocade device supports command authorization and command accounting for CLI commands entered at the console.

AAA support for commands entered at the console includes the following:

- The login prompt that uses AAA authentication, using authentication method lists
- EXEC authorization
- EXEC accounting
- Command authorization
- Command accounting
- System accounting

The **no** form of the command disables the support for AAA commands entered at the console.

NOTE
If you have previously configured the device to perform command authorization using a RADIUS server, entering the **enable aaa console** command may prevent the execution of any subsequent commands entered on the console. This happens because RADIUS command authorization requires a list of allowable commands from the RADIUS server. This list is obtained during RADIUS authentication. For console sessions, RADIUS authentication is performed only if you have configured **aaa authentication enable** and specified RADIUS as the authentication method (for example, with the **aaa authentication enable default radius** command). If RADIUS authentication is never performed, the list of allowable commands is never obtained from the RADIUS server. Consequently, there would be no allowable commands on the console.

Examples

The following example shows how to configure command authorization and command accounting for console commands.

```
device(config)# enable aaa console
```

enable-accounting

Enables Access Control List (ACL) accounting for IPv4 and IPv6 named ACLs.

Syntax

enable-accounting

no enable-accounting

Command Default

This option is disabled.

Modes

IPv4 and IPv6 access-list configuration modes

Usage Guidelines

This is only applicable to named ACLs. The **no** form of this command disables ACL accounting on the associated ACL interface.

Examples

The following example enables IPv6 ACL accounting. The named access-list must be configured before enabling the ACL accounting.

```
device(config)# ipv6 access-list v6
device(config-ipv6-access-list-v6)# enable-accounting
```

The following example enables ACL accounting for an IPv4 named ACL.

```
device(config)# ip access-list standard std
device(config-std-nacl)# permit 10.10.10.0/24
device(config-std-nacl)# deny 10.20.20.0/24
device(config-std-nacl)# enable-accounting
```

History

Release version	Command history
08.0.10	This command was introduced.

enable acl-per-port-per-vlan

Applies an inbound IPv4 ACL to specific VLAN members on a port (Layer 2 devices only) or to specific ports on a virtual interface (VE) (Layer 3 devices only).

Syntax

enable acl-per-port-per-vlan

no enable acl-per-port-per-vlan

Command Default

By default, an inbound IPv4 ACL is not applied to specific VLAN members on a port.

Modes

Global configuration mode

Usage Guidelines

This command is applicable to IPv4 ACLs only. IPv6 ACLs do not support ACL filtering based on VLAN membership or VE port membership. This command is not applicable to outbound traffic.

IPv4 ACLs that filter based on VLAN membership or VE port membership (ACL per port per VLAN), are supported together with IPv6 ACLs on the same device, as long as they are not bound to the same port or virtual interface.

The **enable acl-per-port-per-vlan** command must be followed by the **write-memory** and **reload** commands to place the change into effect.

The **no** form of the command disables the application of an inbound IPv4 ACL to a specific VLAN.

Examples

The following example applies an inbound IPv4 ACL to specific VLAN members on a port.

```
device(config)# enable acl-per-port-per-vlan
device(config)# write memory
device(config)# exit
device# reload
```

enable egress-acl-on-control-traffic

Enables applying outbound ACLs to traffic generated by the CPU.

Syntax

enable egress-acl-on-control-traffic

no enable egress-acl-on-control-traffic

Command Default

By default, outbound ACLs are not applied to traffic generated by the CPU.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets to the default; that is, outbound ACLs are not applied to traffic generated by the CPU.

Examples

The following example shows how to apply outbound ACLs to traffic generated by the CPU.

```
device(config)# enable egress-acl-on-control-traffic
```

enable (GVRP)

Enables GVRP on ports.

Syntax

enable { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no enable { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

GVRP is not enabled on ports.

Parameters

all

Enables GVRP on all ports.

ethernet *stackid/slot/port*

Enables GVRP on the specified port.

to *stackid/slot/port*

Specifies the range of ports upon which to enable GVRP.

Modes

GVRP configuration mode

Usage Guidelines

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

Examples

The following example shows how to enable GVRP on all ports.

```
device(config)# gvrp-enable
device(config-gvrp)# enable all
```

The following example shows how to enable GVRP on a list of specific ports.

```
device(config)# gvrp-enable
device(config-gvrp)# enable ethernet 1/1/24 ethernet 1/2/24 ethernet 1/4/17
```

The following example shows how to enable GVRP on a range of ports.

```
device(config)# gvrp-enable
device(config-gvrp)# enable ethernet 1/1/1 to 1/1/8
```

The following example shows how to enable GVRP on a range of ports and a list of ports.

```
device(config)# gvrp-enable
device(config-gvrp)# enable ethernet 1/1/1 to 1/1/8 ethernet 1/1/24 ethernet 1/6/24 ethernet 1/8/17
```

enable (LAG)

Enables an individual port within a LAG.

Syntax

enable port-name *name*

enable ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

Ports within a LAG are not enabled.

Parameters

port-name *name*

Enables a named port within a LAG.

ethernet *stackid/slot/port*

Enables the specified Ethernet port within the LAG.

to *stackid/slot/port*

Enables a range of ports within the LAG.

Modes

LAG configuration mode

Usage Guidelines

To enable a port belonging to a keep-alive LAG, you must use the **enable** command from the interface configuration mode.

Examples

The following example shows how to enable a port within a LAG configuration.

```
device(config)# lag blue static
device(config-lag-blue)# deploy
device(config-lag-blue)# enable ethernet 1/3/1
```

The following example shows how to enable a port within a LAG configuration.

```
device(config)# lag blue static
device(config-lag-blue)# deploy
device(config-lag-blue)# enable port-name port1
```

The following example shows how to enable a port belonging to a keep-alive LAG.

```
device(config)# lag test keep-alive
device(config-lag-test)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# enable
```

enable (MRP)

Enables the metro ring.

Syntax

enable

no enable

Command Default

The metro ring is disabled by default.

Modes

Metro ring configuration mode

Usage Guidelines

The **no** form of the command disables the metro ring.

Examples

The following example enables the metro ring.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)# enable
```

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 *device/slot/port*

no enable-mka ethernet *device/slot/port*

Command Default

MKA is not enabled on an interface.

Parameters

ethernet *device/slot/port*

Specifies an Ethernet interface and the number of the device, the slot on the device, and the port on that slot.

Modes

dot1x-mka-interface mode

Usage Guidelines

When the **no** version of the command is executed, MACSec is removed from the port.

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

For a MACsec channel to be created between two ports, both ports and devices designated must have MACsec enabled and configured.

Examples

The following example enables MACsec on port 2, slot 3 of the first device in the stack.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# enable-mka ethernet 1/3/2
device(config-dot1x-mka-1/3/2)#
```

History

Release version	Command history
08.0.20	This command was introduced.

enable (Port)

Activates or enables a port.

Syntax

enable

Command Default

The port is enabled (active).

Modes

Interface configuration mode

Usage Guidelines

A port can be made inactive (disabled) or active (enabled) by selecting appropriate status option.

Examples

The following example shows how to enable or activate a disabled port.

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

enable (MAC Port Security)

Enables MAC port security.

Syntax

enable

no enable

Command Default

By default, MAC port security is disabled on all interfaces.

Modes

Port security configuration mode

Port security interface configuration mode

Usage Guidelines

The **no** form of the command disables the MAC port security.

Examples

The following example enables MAC port security on all interfaces.

```
device(config)# port security
device(config-port-security)# enable
```

The following example enables MAC port security on a specific interface.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# port security
device(config-port-security-e1000-1/1/1)# enable
```

enable nd hop-limit

For an IPv6 ACL, enables dropping neighbor discovery (ND) packets for which the hop limit is less than 255.

Syntax

enable nd hop-limit

no enable nd hop-limit

Command Default

Hop-limit check for neighbor discovery (ND) packets is disabled.

Modes

IPv6 ACL configuration mode

Usage Guidelines

Checking for ND packets with hop limit less than 255 helps protect the device from denial of service (DoS) attacks.

ACLs enabled for hop-limit check are effective only when applied to interfaces. (If you configure an ACL that is already applied to an interface, there is no need to re-apply it.)

This command is effective in ACLs applied to all types of supported interface—physical, port-channel, and VE.

This command applies to the following types of ND packets:

- neighbor advertisement (NA)
- neighbor solicitation (NS)
- router advertisement (RA)
- router solicitation (RS)

To disable hop-limit check for ND packets, use the **no** form of this command.

Examples

The following example enables hop-limit check for the IPv6 ACL being configured.

```
device# configure terminal
device(config)# ipv6 access-list hl_acl
device(config-ipv6-access-list hl_acl)# enable nd hop-limit
```

The following example disables hop-limit check for the IPv6 ACL being configured.

```
device# configure terminal
device(config)# ipv6 access-list hl_acl
device(config-ipv6-access-list hl_acl)# no enable nd hop-limit
```

Release version	Command history
08.0.61	This command was introduced.
08.0.30p	Support for this command for ICX 7000 series devices was added.

enable password-display

Enables the display of the community string.

Syntax

enable password-display

no enable password-display

Command Default

The display of the community string is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **enable password-display** command enables display of the community string in the output of the **show snmp server** command. Display of the community string remains encrypted in the startup-config and running-config files. When the **enable password-display** command is configured, the user password and SNMP community string are encrypted in the **show run** command output.

The **no** form of the command disables the display of the community string in the output of the **show snmp server** command.

Examples

The following example shows how to enable the display of the community string.

```
device(config)# enable password-display
```

enable password-min-length

Configures the minimum length on the Line (Telnet), Enable, or Local passwords.

Syntax

enable password-min-length *length*

no enable password-min-length *length*

Command Default

The password length is one character.

Parameters

length

The number of characters or the length of the password. The range is from 1 through 48. The default is 1.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the password length to the default.

Examples

The following example shows how to specify that the Line, Enable, and Local passwords be at least 8 characters.

```
device(config)# enable password-min-length 8
```

enable port-config-password

Allows read-and-write access for specific ports but not for global (systemwide) parameters.

Syntax

enable port-config-password [*password*]

no enable port-config-password [*password*]

Command Default

Read-write access for specific ports is not configured.

Parameters

password

Alphanumeric password string.

Modes

Global configuration mode

Usage Guidelines

You can set one password for each of the management privilege levels: Super User level, Port Configuration level, and Read Only level.

You also can configure up to 16 user accounts consisting of a username and password, and assign each user account to one of the three privilege levels.

NOTE
You must set the Super User level password before you can set other types of passwords.

NOTE
You must use the CLI to assign a password for management privilege levels. You cannot assign a password using the Web Management Interface.

The **no** form of the command removes the configured password access.

Examples

The following example shows how to set Port Configuration level password.

```
device(config)# enable port-config-password password1
```

enable read-only-password

Allows access to the Privileged EXEC mode and User EXEC mode of the CLI, but only with read access.

Syntax

enable read-only-password [*password*]

no enable read-only-password [*password*]

Command Default

Read access for the Privileged EXEC and User EXEC modes of the CLI is not configured.

Parameters

password

Alphanumeric password string.

Modes

Global configuration mode

Usage Guidelines

You can set one password for each of the management privilege levels: Super User level, Port Configuration level, and Read Only level.

You also can configure up to 16 user accounts consisting of a username and password, and assign each user account to one of the three privilege levels.

NOTE
You must set the Super User level password before you can set other types of passwords.

NOTE
You must use the CLI to assign a password for management privilege levels. You cannot assign a password using the Web Management Interface.

The **no** form of the command removes the configured password access.

Examples

The following example shows how to set Read Only level password.

```
device(config)# enable read-only-password password1
```

enable snmp

Enables SNMP access modes.

Syntax

enable snmp { **config-tacacs** | **config-radius** | **ve-statistics** }

no enable snmp { **config-tacacs** | **config-radius** | **ve-statistics** }

Command Default

The SNMP access modes for TACACS and RADIUS are disabled.

Parameters

config-tacacs
Enables TACACS configuration access mode.

config-radius
Enables RADIUS configuration access mode.

ve-statistics
Enables the display of virtual port statistics.

Modes

Global configuration mode

Usage Guidelines

To configure TACACS, TACACS+ or RADIUS authentication parameters, you must enable the corresponding SNMP access mode.

The **no** form of the command disables the SNMP access modes.

Examples

The following example shows how to enable the SNMP access mode for TACACS.

```
device(config)# enable snmp config-tacacs
```

The following example shows how to enable the SNMP access mode for RADIUS.

```
device(config)# enable snmp config-radius
```

The following example shows how to enable the display of virtual port statistics.

```
device(config)# enable snmp ve-statistics
```

enable strict-password-enforcement

Enables the password security feature.

Syntax

enable strict-password-enforcement

no enable strict-password-enforcement

Command Default

Strict password is not enforced.

Modes

Global configuration mode

Usage Guidelines

When strict password enforcement is enabled on the Brocade device, you must enter a minimum of eight characters containing the following combinations when you create an enable and a user password:

- At least two uppercase characters
- At least two lowercase characters
- At least two numeric characters
- At least two special characters

NOTE
Password minimum character and combination requirements are strictly enforced.

Passwords must not share four or more concurrent characters with any other password configured on the router. If the you try to create a password with four or more concurrent characters, an error message will be returned.

If you try to configure a password that was previously used, the Local User Account configuration will not be allowed and an error message will be displayed.

The **no** form of the command disables strict password enforcement.

Examples

The following example shows how to enable strict password enforcement.

```
device(config)# enable strict-password-enforcement
```

enable super-user-password

Allows complete read-and-write access to the system.

Syntax

enable super-user-password [*password*]

no enable super-user-password [*password*]

Command Default

Complete read-write access to the system is not configured.

Parameters

password

Alphanumeric password string.

Modes

Global configuration mode

Usage Guidelines

You can set one password for each of the management privilege levels: Super User level, Port Configuration level, and Read Only level. The **enable super-user-password** command is generally for system administrators only. The Super User privilege level allows you to configure passwords.

You also can configure up to 16 user accounts consisting of a username and password, and assign each user account to one of the three privilege levels.

You must set the Super User level password before you can set other types of passwords.

NOTE
You must use the CLI to assign a password for management privilege levels. You cannot assign a password using the Web Management Interface.

The **no** form of the command removes the configured password access.

Examples

The following example shows how to set the Super User level password.

```
device(config)# enable super-user-password password1
```

enable telnet

Configures Telnet access control parameters.

Syntax

enable telnet { **authentication** | **password** *password* }

no enable telnet { **authentication** | **password** *password* }

Command Default

Telnet authentication is not enabled and the Telnet password is not set.

Parameters

authentication
Enables Telnet authentication.

password *password*
Sets a password for Telnet access.

Modes

Global configuration mode

Usage Guidelines

To authenticate Telnet access to the CLI, you also must enable the authentication by entering the **enable telnet authentication** command. You cannot enable Telnet authentication using the Web Management Interface.

The **no** form of the command removes the Telnet authentication or Telnet password.

Examples

The following example shows how to enable Telnet authentication.

```
device(config)# enable telnet authentication
```

The following example shows how to set the password for Telnet access.

```
device(config)# enable telnet password pass1
```

enable user

Configures login and password parameters specific to a user.

Syntax

enable user { **disable-on-login-failure** [*invalid-attempts*] | **password-aging** | **password-history** [*previous-passwords*] | **password-masking** }

no enable user { **disable-on-login-failure** [*invalid-attempts*] | **password-aging** | **password-history** [*previous-passwords*] | **password-masking** }

Command Default

Password masking is not enabled.

Up to three login attempts are allowed.

The Brocade device stores the last five user passwords for each user.

Password aging is disabled.

Parameters

disable-on-login-failure *invalid-attempts*
Specifies the number of login attempts before a user is locked out (disabled). The range is from 1 through 10. The default is 3.

password-aging
Enables password aging.

password-history *previous-passwords*
Specifies how many previous passwords should be stored. The range is from 1 through 15. The default is 5.

password-masking
Enables password masking.

Modes

Global configuration mode

Usage Guidelines

By default, when you use the CLI to create a user password, the password displays on the console as you type it. For enhanced security, you can configure the Brocade device to mask the password characters entered at the CLI. When password masking is enabled, the CLI displays an asterisk (*) on the console instead of the actual password character entered.

For enhanced security, password aging enforces quarterly updates of all user passwords. After 180 days, the CLI automatically prompts users to change their passwords when they attempt to sign on. When password aging is enabled, the software records the system time that each user password was configured or last changed. The time displays in the output of the **show running configuration** command, indicated by set-time.

By default, the Brocade device stores the last five user passwords for each user. When changing a user password, the user cannot use any of the five previously configured passwords. For security purposes, you can configure the Brocade device to store up to 15 passwords for each user, so that users do not use the same password multiple times. If a user attempts to use a password that is stored, the system prompts the user to choose a different password.

The CLI provides up to three login attempts. If a user fails to login after three attempts, that user is locked out (disabled). If desired, you can increase or decrease the number of login attempts before the user is disabled.

Use the **no** form of the command to remove the login and password configurations.

Examples

The following example shows how to set the number of login attempts for a user.

```
device(config)# enable user disable-on-login-failure 10
```

The following example shows how to enable password aging.

```
device(config)# enable user password-aging
```

The following example shows how to enable password masking, and the CLI behavior when configuring the username and password once password masking is enabled.

```
device(config)# enable user password-masking

device(config)# username xyz password
Enter Password: ********
```

The following example shows how to configure the device to store up to 10 previous passwords.

```
device(config)# enable user password-history 10
```

enable (VSRP)

Enables the VSRP VRID for a port-based VLAN.

Syntax

enable

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.

Examples

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

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

enable (Web Authentication)

Enables Web Authentication.

Syntax

enable

no enable

Command Default

Web Authentication is disabled.

Modes

Web Authentication configuration mode

Usage Guidelines

The **no** form of the command disables Web Authentication.

Examples

The following example enables Web Authentication on VLAN 10.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# enable
```

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-router)# enforce-first-as
```

erase flash

Erases the image stored in the flash of the system.

Syntax

erase flash { **primpary** | **secondary** | **unit-id-pri** *string* | **unit-id-sec** *string* }

Parameters

primary

Erases the image on the primary code image.

secondary

Erases secondary code image.

unit-id-pri *string*

Erases the primary code image from the specified stack member. You can specify **all** or a member list (2,3,5-7) without blank spaces.

unit-id-sec *string*

Erases the secondary code image from the specified stack member. You can specify **all** or a member list (2,3,5-7) without blank spaces.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to erase the files stored in the primary, secondary flash or on the stack units.

Examples

The following example erases the image stored in secondary flash of the system.

```
device# erase flash secondary
```

The following example erases the image stored in secondary flash of a set of stack units.

```
device# erase flash unit-id-sec 3,4,5-8,9
```

erase startup-config

Erases the startup configuration.

Syntax

erase startup-config [**unit-id** *unit-list*]

Parameters

unit-id *unit-list*

Erases the stratup configuration file from the specified stack member. You can specify a member list (2,3,5-7) without blank spaces.

Modes

Privileged EXEC mode

Examples

The following example erases the startup configuration from a members in a stack.

```
device# erase startup-config unit-id 2,5,7-8,10
```

errdisable packet-inerror-detect

Enables the device to monitor configured ports for inError packets and defines the sampling time interval in which the number of inError packets is counted.

Syntax

errdisable packet-inerror-detect *sampling-interval*

no errdisable packet-inerror-detect *sampling-interval*

Command Default

There is no monitoring for inError packets on any port of the device.

Parameters

sampling-interval

Specifies the sampling interval in seconds. It can take a value in the inclusive range of 2 through 60 seconds.

Modes

Global configuration mode

Usage Guidelines

If the number of inError packets exceeds the configured threshold for two consecutive sampling windows, then the configured port is error-disabled. The **no** form of this command disables this monitoring.

Examples

The following example sets the sampling interval in which the number of inError packets is counted to three seconds.

```
device(config)# errdisable packet-inerror-detect 3
```

History

Release version	Command history
07.3.00g	This command was introduced.

errdisable recovery

Enables a port to recover automatically from the error-disabled state.

Syntax

errdisable recovery cause { **all** | *cause* }

no errdisable recovery cause { **all** | *cause* }

errdisable recovery interval *time*

no errdisable recovery interval *time*

Command Default

The ports in the error-disabled state are not recovered.

Parameters

all

Enables the ports to automatically recover from an error-disabled state caused by reasons such as BPDU guard violation, the number of inError packets exceeding the configured threshold, a loop-detection violation, or due to reception of a critical event from the remote device in the case of EFM-OAM interface.

cause

Configures the ports to recover from an error-disabled state caused by a specific reason which can be any of the following:

- **bpduguard**
- **loam-critical-event**
- **loop-detection**
- **packet-inerror-detect**
- **pvstplus-protect**

bpduguard

Configures the port to recover from the error-disabled state if the state was caused because of BPDU guard violation.

loam-critical-event

Configures the EFM-OAM interface to recover from the error-disabled state if the state was caused due to reception of a critical event from the remote device.

loop-detection

Configures the port to recover from the error-disabled state if the state was caused because of loop detection.

packet-inerror-detect

Configures the port to recover from the error-disabled state if the state was caused because the number of inError packets exceeded the configured threshold.

pvstplus-protect

Configures the port to recover from the error-disabled state if the state was caused because the PVST+ Protect feature is enabled.

interval

Configures a timeout value for the recovery mechanism when the port is in an error-disabled state. Upon the expiry of the timeout value, the ports are automatically recovered.

time

Specifies the recovery time interval in seconds for the device to wait before automatically recovering the ports. The valid values are from 10 through 65535 seconds. The default recovery timeout value is 300 seconds.

Modes

Global configuration mode

Usage Guidelines

When automatic recovery re-enables the port, the port is not in the error-disabled state, but it can remain down for other reasons, such as the Tx/Rx of the fibre optic not being seated properly. Thus, the port is not able to receive the signal from the other side. In this case, after the optic is inserted correctly, you should manually disable the port and then enable it.

The **no** form of the **errdisable recovery cause** command disables the error-disabled recover functionality.

The **no** form of the **errdisable recovery interval** command reverts to the default recovery time interval value.

Examples

The following example configures the device to recover the port from the error-disabled state caused because of BPDU guard violation.

```
device(config)# errdisable recovery bpduguard
```

The following example configures the device to recover the EFM-OAM interface from the error-disabled state caused by reception of a critical event from the remote device.

```
device(config)# errdisable recovery loam-critical-event
```

The following example configures the device to recover the port from the error-disabled state caused because of loop detection.

```
device(config)# errdisable recovery loop-detection
```

The following example configures the device to recover the port from the error-disabled state caused because the number of inError packets exceeded the configured threshold.

```
device(config)# errdisable recovery packet-inerror-detect
```

The following example configures the device to recover the port from the error-disabled state caused because the number of inError packets exceeded the configured threshold.

```
device(config)# errdisable recovery pvstplus-protect
```

The following example configures the error-disabled recovery timeout interval as 120 seconds.

```
device(config)# errdisable recovery interval 120
```

History

Release version	Command history
08.0.30	The **loam-critical-event** option was introduced.
08.0.30mb	The **pvstplus-protect** option was introduced.

ethernet (EFM-OAM)

Enables or disables EFM-OAM on an interface or multiple interfaces.

Syntax

ethernet *stackid/slot/port* [[**to** *stackid/slot/port*] [**ethernet** *stackid/slot/port*] ...] { **active** | **passive** | **allow-loopback** | **remote-failure critical-event action block-interface** }

no ethernet *stackid/slot/port* [[**to** *stackid/slot/port*] [**ethernet** *stackid/slot/port*] ...] { **active** | **passive** | **allow-loopback** | **remote-failure critical-event action block-interface** }

Command Default

The EFM-OAM is disabled locally on an interface.

Parameters

ethernet *stackid/slot/port*
Specifies the interface.

to
Configures the range of interfaces to enable EFM-OAM.

active
Sets the EFM-OAM operational mode as active on the interface.

passive
Sets the EFM-OAM operational mode as passive on the interface.

allow-loopback
Enables the interface to respond to a loopback request from the remote device.

remote-failure critical-event action block-interface
Configures the device to block the remote interface upon reception of a critical event information from the remote interface.

Modes

EFM-OAM protocol configuration mode

Usage Guidelines

When the active mode is specified, the device can send OAMPDU packets over the port to initiate an EFM-OAM discovery process. For the discovery process to be initiated, the EFM-OAM protocol must be enabled.

When the passive mode is specified, the device cannot use the port to send OAMPDU packets, but can respond if it receives OAMPDUs from the remote device.

When both peers are in passive mode (abnormal configuration), EFM-OAM protocol will not converge.

The OAMPDUs and pause frames will not be looped back in the loopback mode. All other Layer 2 protocol packets will be looped back if received on a loopbacked interface.

The **no** form of the command disables the EFM-OAM locally on the specified interface.

Examples

The following example enables EFM-OAM on an interface and sets it to active mode.

```
device(config)# link-oam
device(config-link-oam)# ethernet 1/1/3 active
```

The following example enables EFM-OAM on a range of interfaces and sets them to active mode.

```
device(config)# link-oam
device(config-link-oam)# ethernet 1/1/4 to 1/1/8 active
```

The following example enables EFM-OAM on an interface and sets it to passive mode.

```
device(config)# link-oam
device(config-link-oam)# ethernet 2/1/1 passive
```

The following example enables EFM-OAM on a range of interfaces and sets them to passive mode.

```
device(config)# link-oam
device(config-link-oam)# ethernet 2/1/1 to 2/1/6 passive
```

The following example configures the interface to respond to the loopback request from the remote device.

```
device(config)# link-oam
device(config-link-oam)# ethernet 1/1/3 allow-loopback
```

The following example sets the device to block the interface when a critical event failure condition is detected.

```
device(config)# link-oam
device(config-link-oam)# ethernet 2/1/1 remote-failure critical-event action block-interface
```

History

Release version	Command history
08.0.30	This command was introduced.

ethernet loopback

Enables the Ethernet loopback functionality on a port in the VLAN-unaware mode.

Syntax

ethernet loopback

no ethernet loopback

Command Default

Ethernet loopback is not enabled on a port.

Modes

Interface configuration mode

Usage Guidelines

The Ethernet loopback functionality on a port in the VLAN-unaware mode can be configured either as flow-aware or flow-unaware. The specified port does not need to be explicitly assigned as a member of any VLAN.

To enable Ethernet loopback on a port in the VLAN-unaware mode as flow-aware, the **ethernet loopback test-mac** command must be executed before enabling the Ethernet loopback. The **ethernet loopback test-mac** command is mandatory on Brocade ICX 7750, Brocade ICX 7450, and Brocade ICX 7250 devices. To enable Ethernet loopback on these devices, you must first configure the **ethernet loopback test-mac** command. In other supported platforms, the **ethernet loopback test-mac** command is optional to enable Ethernet loopback.

To add or delete a port from VLAN, the VLAN unaware ethernet loopback configuration on the port must be removed.

Before adding or deleting a port form VLAN, the VLAN unaware ethernet configuration must be removed, if configured.

The **ethernet loopback** command is not supported on multiple ports (MIF) mode.

The **no** form of the command disables the Ethernet loopback functionality on the specified port.

Examples

The following example configures Ethernet loopback on a specific port in the VLAN-unaware mode as flow-unaware.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ethernet loopback
```

The following example configures Ethernet loopback in VLAN-unaware mode as flow-aware.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ethernet loopback test-mac 1111.2222.3333 4444.5555.5555
device(config-if-e1000-1/1/1)# ethernet loopback
```

The following example shows the error which occurs when you try to add a port to VLAN, without removing the VLAN unaware ethernet loopback configuration.

```
bkes_oct14-16_DND(config-if-e1000-3/1/4)#vlan 10
bkes_oct14-16_DND(config-vlan-10)#tag eth 3/1/4
Error: Port 3/1/4 has Ethernet loopback configuration
Note: Remove Ethernet loopback from port 3/1/4 and then add port as member of VLAN 10
bkes_oct14-16_DND(config-vlan-10)#int eth 3/1/4
```

History

Release version	Command history
08.0.30	This command was introduced.

ethernet loopback (VLAN-aware)

Configures the Ethernet loopback functionality on one or a set of ports in a specific VLAN (VLAN-aware mode).

Syntax

ethernet loopback ethernet *stackid/slot/port* [[**to** *stackid/slot/port*] [**ethernet** *stackid/slot/port*]...]

no ethernet loopback ethernet *stackid/slot/port* [[**to** *stackid/slot/port*] [**ethernet** *stackid/slot/port*]...]

Command Default

Ethernet loopback is not enabled on any port in a VLAN.

Parameters

ethernet
Specifies the Ethernet interface.

to
Configures the range of ports.

stackid/slot/port
Specifies the interface details.

Modes

VLAN configuration mode

Usage Guidelines

The Ethernet loopback functionality on a port in the VLAN-aware mode can be configured either as flow-aware or flow-unaware. The ports on which Ethernet loopback is being enabled must be explicitly assigned as a member of the VLAN.

To enable Ethernet loopback on a port in the VLAN-aware mode as flow-aware, the **ethernet loopback test-mac** command must be executed for the specific port from the interface mode before enabling Ethernet loopback. The **ethernet loopback test-mac** command is mandatory on Brocade ICX 7750, Brocade ICX 7450, and Brocade ICX 7250 devices. To enable Ethernet loopback on these devices, you must first configure the **ethernet loopback test-mac** command. In other supported platforms, the **ethernet loopback test-mac** command is optional to enable Ethernet loopback.

Enable **acl-per-port-per-vlan** configuration before issuing the ethernet loopback command. If not enabled, an error message "Error - Enable **acl-per-port-per-vlan** and configure VLAN unaware ethernet loopback" prompts you to enable the configuration.

A port cannot be configured as VLAN-aware and VLAN-unaware simultaneously, and the flow configuration must be either flow-aware or flow-unaware.

The **ethernet loopback** command in VLAN-aware mode is not supported on VLAN Group, VLAN Range, or mult-range VLAN (MVLAN) mode.

The **ethernet loopback** command VLAN-aware mode cannot be configured on a set of VLANs that share a Layer 2 topology (Topology Group).

The **no** form of the command disables Ethernet loopback from the ports of the specified VLAN.

Examples

The following example configures Ethernet loopback in VLAN-aware mode as flow-aware.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ethernet loopback test-mac 1111.2222.3333 4444.5555.5555
device(config-if-e1000-1/1/1)# exit
device(config)# vlan 100
device(config-vlan-100)# ethernet loopback ethernet 1/1/1 to 1/1/10
```

The following example configures Ethernet loopback on a port in VLAN-aware mode as flow-unaware.

```
device(config)# vlan 100
device(config-vlan-100)# ethernet loopback ethernet 1/1/1
```

The following example configures Ethernet loopback on a range of ports in VLAN-aware mode as flow-unaware.

```
device(config)# vlan 100
device(config-vlan-100)# ethernet loopback ethernet 1/1/1 to 1/1/10
```

The following example configures Ethernet loopback on two separate ports in VLAN-aware mode as flow-unaware.

```
device(config)# vlan 100
device(config-vlan-100)# ethernet loopback ethernet 1/1/1 ethernet 1/2/3
```

History

Release version	Command history
08.0.30	This command was introduced.

ethernet loopback test-mac

Configures the port as flow-aware by specifying the source and destination MAC addresses of the flow on the interface.

Syntax

ethernet loopback test-mac *destination-MAC source-MAC*

no ethernet loopback test-mac *destination-MAC source-MAC*

Command Default

The port is flow-unaware.

Parameters

destination-MAC

Specifies the flow parameter destination MAC address of the traffic.

source-MAC

Specifies the flow parameter source MAC address of the traffic.

Modes

Interface configuration mode

Usage Guidelines

You must configure the **ethernet loopback test-mac** command on Brocade ICX 7750, Brocade ICX 7450, and Brocade ICX 7250 devices before enabling Ethernet loopback. In other supported platforms, configure the **ethernet loopback test-mac** command only if you require the port to be flow-aware.

The source MAC address and destination MAC address must be unicast MAC addresses and the source MAC address must be unique across the network for proper Ethernet loopback operation.

You cannot configure a port as flow-aware and flow-unaware simultaneously. The flow can be configured on an in-service Ethernet loopback port. However, the flow configuration cannot be modified or removed if there is an ongoing loopback service on the interface.

The **ethernet loopback test-mac** command is not supported in multi-range VLAN (MVLAN) mode.

The **no** form of the command removes the flow configuration for the specified port.

Examples

The following example configures the flow on a specific port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ethernet loopback test-mac 1111.2222.3333/4444.5555.5555
```

History

Release version	Command history
08.0.30	This command was introduced.

excluded-address

Specifies the addresses that should be excluded from the address pool.

Syntax

excluded-address { *address* | *address-low address-high* }

Parameters

address
Specifies a single address.

address-low address-high
Specifies a range of addresses.

Modes

DHCP server pool configuration mode.

Usage Guidelines

Use this command to specify either a single address or a range of addresses that are to be excluded from the address pool.

Examples

The following example specifies the excluded address.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# excluded-address 10.2.3.44
```

exclude ethernet

Excludes a port from the protocol VLAN membership.

Syntax

exclude ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no exclude ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

The port is not excluded from the protocol VLAN membership.

Parameters

stackid/slot/port
Specifies the Ethernet port which should be excluded from the static protocol VLAN membership.

to *stackid/slot/port*
Specifies the range of ports that should be exluded from the static protocol VLAN membership.

Modes

IP protocol VLAN configuration mode

IPX protocol VLAN configuration mode

IPv6 protocol VLAN configuration mode

AppleTalk protocol VLAN configuration mode

DECnet protocol VLAN configuration mode

NetBIOS protocol VLAN configuration mode

Other protocol VLAN configuration mode

Usage Guidelines

The **no** form of the command includes in the protocol VLAN membership.

Examples

The following example shows how to exclude ports from the protocol VLAN memebership.

```
device(config)# vlan 10
device(config-vlan-10)# atalk-proto name Red
device(config-atalk-proto)# no dynamic
device(config-atalk-proto)# exclude ethernet 1/1/1 to 1/1/3
```

Commands F - J

failover

Enables or disables LAG (Link Aggregation Group) hardware failover on the next port in LAG or on all ports in LAG.

Syntax

failover {**next** | **all**}

no failover {**next** | **all**}

Command Default

LAG hardware failover is disabled.

Parameters

next

Specifies that failover is to be enabled or disabled on the next port in LAG.

all

Specifies that failover is to be enabled or disabled on all ports in LAG.

Modes

Dynamic LAG configuration mode

Usage Guidelines

The **no** form of this command disables LAG hardware failover.

LAG hardware failover is supported only on Brocade ICX 7750 devices.

Examples

The following example enables LAG failover on the next port in LAG:

```
device(config)# lag one dynamic
device(config-lag-one)# failover next
```

The following example enables LAG failover on all ports in LAG:

```
device(config)# lag one dynamic
device(config-lag-one)# failover all
```

History

Release version	Command history
08.0.10	This command was introduced.

fast-external-fallover

Resets the session if a link to an EBGP peer goes down.

Syntax

fast-external-fallover

no fast-external-fallover

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-router)# fast-external-fallover
```

fast port-span

Enables Fast Port Span, configuring the ports attached to the end stations to enter into the forwarding state in four seconds.

Syntax

fast port-span [**exclude ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]]

no fast port-span [**exclude ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]]

Command Default

Fast Port Span is enabled by default on all ports that are attached to end stations.

Parameters

exclude

Excludes a port from Fast Port Span while leaving Fast Port Span enabled globally.

ethernet *stackid/slot/port*

Specifies the Ethernet port that you want to exclude from Fast Port Span.

to *stackid/slot/port*

Specifies a range of Ethernet ports that you want to exclude from Fast Port Span.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

Disabling and then re-enabling Fast Port Span clears the exclude settings and thus enables Fast Port Span on all eligible ports. To make sure Fast Port Span remains enabled on the ports following a system reset, save the configuration changes to the startup-config file after you re-enable Fast Port Span. Otherwise, when the system resets, those ports will again be excluded from Fast Port Span.

Fast Port Span allows faster convergence on ports that are attached to end stations and thus do not present the potential to cause Layer 2 forwarding loops. Because the end stations cannot cause forwarding loops, they can safely go through the STP state changes (blocking to listening to learning to forwarding) more quickly than is allowed by the standard STP convergence time. Fast Port Span performs the convergence on these ports in four seconds (two seconds for listening and two seconds for learning).

Fast Port Span is a system-wide parameter and is enabled by default. Thus, when you boot a device, all the ports that are attached only to end stations run Fast Port Span. For ports that are not eligible for Fast Port Span, such as ports connected to other networking devices, the device automatically uses the normal STP settings.

The **no** form of the command disables Fast Port Span. Using the **exclude** option with the **no** form of the command enables Fast Port Span on the specified ports.

Examples

The following example enables Fast Port Span on all ports.

```
device(config)# fast port-span
```

The following example excludes a set of ports from Fast Port Span.

```
device(config)# fast port-span exclude ethernet 1/1/1 ethernet 1/2/1 ethernet 1/3/1
```

The following example shows how to re-enable Fast Port Span on port 1/1/1 only while not re-enabling other excluded ports.

```
device(config)# no fast port-span exclude 1/1/1
```

The following example shows how to re-enable Fast Port Span on all excluded ports.

```
device(config)# no fast port-span
device(config)# fast port-span
device(config)# write memory
```

fast uplink-span

Enables Fast Uplink Span, configuring a device deployed as a wiring closet switch to decrease the convergence time for the uplink ports to another device to just one second.

Syntax

fast uplink-span ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no fast uplink-span ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

Fast Uplink Span is not enabled.

Parameters

ethernet *stackid/slot/port*
Specifies the Ethernet port on which you want to enable Fast Uplink Span.

to *stackid/slot/port*
Specifies a range of ports on which you want to enable Fast Uplink Span.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

The new uplink port goes directly to forward mode (bypassing listening and learning modes). The wiring closet switch must be a Brocade device, but the device at the other end of the link can be a Brocade device or another vendor's switch.

To configure Fast Uplink Span, specify a group of ports that have redundant uplinks on the wiring closet switch (Brocade device). If the active link becomes unavailable, Fast Uplink Span transitions the forwarding to one of the other redundant uplink ports in just one second. All Fast Uplink Span-enabled ports are members of a single Fast Uplink Span group.

To avoid the potential for temporary bridging loops, Brocade recommends that you use Fast Uplink Span only for wiring closet switches (switches at the edge of the network cloud). In addition, enable Fast Uplink Span only on a group of ports intended for redundancy, so that at any given time only one of the ports is expected to be in the forwarding state.

The **no** form of the command removes Fast Uplink Span on the ports.

Examples

The following example configures a group of ports for Fast Uplink Span.

```
device(config)# fast uplink-span ethernet 1/4/1 to 1/4/4
```

The following example configures Fast Uplink Span for a VLAN.

```
device(config)# vlan 10
device(config-vlan-10)# untag ethernet 1/8/1 to 1/8/2
device(config-vlan-10)# fast uplink-span ethernet 1/8/1 to 1/8/2
```

fdp advertise

Configures the IP management address to advertise.

Syntax

fdp advertise { **ipv4** | **ipv6** }

no fdp advertise { **ipv4** | **ipv6** }

Command Default

When FDP is enabled, by default, the device advertises one IPv4 address and one IPv6 address to its FDP neighbors.

Parameters

ipv4

Configures the IPv4 management address to advertise.

ipv6

Configures the IPv6 management address to advertise.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command sets the device to the default setting.

When FDP is enabled, by default, the device advertises one IPv4 address and one IPv6 address to its FDP neighbors. If desired, you can configure the device to advertise only the IPv4 management address or only the IPv6 management address. You can set the configuration globally on a Layer 2 switch, or on an interface on a Layer 3 switch.

Examples

The following example shows how to set the IPv6 management address to advertise.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# fdp advertise ipv6
```

fdp enable

Enables Foundry Discovery Protocol (FDP) on an interface.

Syntax

fdp enable

no fdp enable

Command Default

FDP is enabled at the interface level once FDP is enabled on the device.

Modes

Interface configuration mode

Usage Guidelines

When FDP is enabled globally, you can disable and re-enable FDP on individual ports.

The **no** form of the command disables FDP on an interface.

Examples

The following example enables FDP on an interface.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# fdp enable
```

fdp holdtime

Configures the Foundry Discovery Protocol (FDP) update hold time.

Syntax

fdp holdtime *secs*

no fdp holdtime *secs*

Command Default

By default, a device that receives an FDP update holds the information until the device receives a new update or 180 seconds have passed since receipt of the last update.

Parameters

secs

Specifies the number of seconds the device that receives an FDP update can hold the update before discarding it. The number of seconds can range from 10 to 255 seconds. The default value is 180 seconds.

Modes

Global configuration mode

Usage Guidelines

Once the device encounters a new update or if 180 seconds have passed since receipt of the last update, the device discards the update.

The **no** form of the command sets the hold time to its default value of 180 seconds.

Examples

The following example sets the hold time to 200 seconds.

```
device(config)# fdp holdtime 200
```

fdp run

Enables a device to globally send FDP packets.

Syntax

fdp run

no fdp run

Command Default

FDP is disabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the device to send FDP packets.

Examples

The following example enables FDP globally.

```
device(config)# fdp run
```

fdp timer

Configures the Foundry Discovery Protocol (FDP) update timer.

Syntax

fdp timer *secs*

no fdp timer *secs*

Command Default

By default, a device enabled for FDP sends an FDP update every 60 seconds.

Parameters

secs

Specifies the number of seconds between updates. The value can range from 5 to 900 seconds. The default value is 60 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command sets the FDP timer to its default value of 60 seconds.

Examples

The following example sets the FDP timer to 360 seconds.

```
device(config)# fdp timer 360
```

filter-strict-security enable

Enables or disables strict filter security for MAC authentication and 802.1X authentication.

Syntax

filter-strict-security

no filter-strict-security

Command Default

Strict filter security is enabled.

Modes

Authentication mode

Usage Guidelines

When strict security mode is enabled, authentication for a port fails if the Filter-Id attribute contains invalid information, or if insufficient system resources are available to implement the IP ACLs.

When strict security mode is enabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, IP ACL configured on the device), then the client will not be authorized, regardless of any other information in the message (for example, if the Tunnel-Private-Group-ID attribute specifies a VLAN on which to assign the port).
- If the device does not have the system resources available to dynamically apply a filter to a port, then the client will not be authenticated.

When strict filter security is disabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, a MAC address filter or IP ACL configured on the device), then the client remains authorized and no filter is dynamically applied to it.
- By default, strict security mode is enabled for all MAC authentication and 802.1X-enabled interfaces, but you can manually disable or enable it using the **filter-strict-security** command from the authentication configuration mode or using the **authentication filter-strict-security** command from the interface configuration mode.

The **no** form of the command disables strict filter security.

Examples

The following example enables strict filter security.

```
device(config)# authentication
device(config-authen)# filter-strict-security enable
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.30mb	This command was modified.

fitrace modules flexauth submodule

Enables debugging for specific modules in the Flexible Authentication feature.

Syntax

fitrace modules flexauth submodule { **vlan** | **filters** | **events** | **packets** | **timers** | **misc** }

no fitrace modules flexauth submodule { **vlan** | **filters** | **events** | **packets** | **timers** | **misc** }

Parameters

vlan
Enables logging for VLAN-operations specific debug messages.

filters
Enables logging for filter-specific debug messages.

events
Enables logging for flexauth-events specific debug messages.

packets
Enables logging for RX/TX-packet specific debug messages.

timers
Enables logging for timer-specific debug messages.

misc
Enables logging for any general unclassified debug messages.

Modes

Global configuration mode

Usage Guidelines

The **no** version of this command deactivates the logging for the specified module.

Diagnostic commands are developed and intended for specialized troubleshooting. Brocade recommends that you work closely with Brocade Technical Support in executing **debug** or **show system internal** commands and interpreting their results.

More than one module can be activated.

Examples

Typical command example

```
device# configure terminal
device(config)# fitrace modules flexauth submodule vlan
```

History

Release version	Command history
08.0.30j	This command was introduced.

flash

Use the **flash** command to perform basic flash file maintenance.

Syntax

flash { **copy** *source-file destination-file* | **dbgflock** | **delete** *flash-file* | **files** *directory-name* | **rename** *source-file destination-file* }

Command Default

N/A

Parameters

copy *source-file destination-file*
: Copy the source flash file to a new file

dbgflock
: Display the flash access lock holder

delete *flash-file*
: Delete the flash file

files *directory-name*
: Display flash files in a particular directory

rename *source-file destination-file*
: Rename a flash file

Modes

Exec mode

Usage Guidelines

The command is useful in flash file maintenance.

Examples

In the following example, flash files are displayed.

```
device# flash files
Type       Size   Name
----------------------
F        24108665 primary
F        24108665 secondary
F             610 startup-config.backup
F            2052 startup-config.txt

48219992 bytes 4 File(s) in FI root

     1768706048 bytes free in FI root
     1768706048 bytes free in /
```

The **show flash** command also displays flash file information but with different results.

```
device# show flash
Stack unit 1:
  Compressed Pri Code size = 24108665, Version:08.0.40qT213 (SPR08040q074.bin)
  Compressed Sec Code size = 24108665, Version:08.0.40qT213 (SPR08040q074.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
  Code Flash Free Space = 1768706048
```

History

Release version	Command history
8.0.10	This command was introduced.

flash-timeout

Configures the flash timeout duration.

Syntax

flash-timeout *time*

no flash-timeout *time*

Command Default

The default flash timeout value is 12 minutes.

Parameters

time

Specifies the flash timeout value in minutes and the range is from 12 to 60 minutes.

Modes

Global configuration mode

Usage Guidelines

The new timeout value will be effective from the next flash operation.

The **no** form of the command removes the flash timeout configuration and restores the default value of 12 minutes.

Examples

The following example configures the flash timeout value as 30 minutes.

```
device(config)# flash-timeout 30
```

History

Release version	Command history
08.0.30	This command was introduced.

flow-control

Enables or disables flow control and flow control negotiation, and advertises flow control.

Syntax

flow-control [**neg-on**]

no flow-control [**neg-on**]

Command Default

Flow control is enabled.

Parameters

neg-on

Enables negotiation on an interface.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of this command disables flow control.

On ICX 7750 devices the default packet-forwarding method is cut-through, in which port flow control (IEEE 802.3x) is not supported but priority-based flow control (PFC) is supported. You can configure the **store-and- forward** command in global configuration mode to enable the store-and-forward method for packet-forwarding.

By default, when flow control is enabled globally and auto-negotiation is on, flow control is enabled and advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, flow control is neither negotiated with nor advertised to the peer.

NOTE
Enabling only port auto-negotiation does not enable flow control negotiation. You must use the **flow-control neg-on** command to enable flow-control negotiation.

Examples

The following example disables flow control globally.

```
Device(config)#no flow-control
```

The following example enables flow control on Ethernet ports 0/1/11 to 0/1/15.

```
Device(config)#interface ethernet 0/1/11 to 0/1/15
device(config-mif-0/1/11-0/1/15)#flow-control
```

The following example disables flow control on Ethernet port 1/1/9.

```
Device(config)# interface ethernet 1/1/9
Device(config-if-e1000-1/1/9)no flow-control
```

The following example enables flow-control negotiation on Ethernet interface 1/1/2.

```
Device(config)# interface ethernet 1/1/2
Device(config-if-e1000-1/1/2)flow-control neg-on
```

History

Release version	Command history
08.0.20	This command was modified. Enabling only auto-negotiation does not enable flow-control negotiation.

force-up ethernet

Forces the member port of a dynamic LAG (Link Aggregation Group) to be logically operational even if the dynamic LAG is not operating.

Syntax

force-up ethernet *port*

no force-up ethernet *port*

Command Default

The member ports of a dynamic LAG are logically operational only if the dynamic LAG is operating.

Parameters

port

Specifies the port.

Modes

Dynamic LAG configuration mode

Usage Guidelines

The **no** form of the command causes the specified port to be logically operational only when the dynamic LAG is operating.

When the dynamic LAG is not operational, the port goes to "force-up" mode. In this mode, the port is logically operational, which enables a PXE-capable host to boot from the network using this port. Once the host successfully boots from the network, the dynamic LAG can connect the host to the network with the LAG link. Even if the dynamic LAG fails later, this port is brought back to "force-up" mode and remains logically operational.

A port that is in "force-up" mode has the operational status ("Ope") of "Frc". Use the **show lag** command to display the operational status.

If any port in a dynamic LAG receives an LACPDU, the port in force-up mode leaves force-mode and becomes a member port in the dynamic LAG.

Examples

The following example enables PXE boot support on member port 3/1/1 of a dynamic LAG R4-dyn.

```
device(config)# lag R4-dyn
device(config-lag-R4-dyn)# force-up ethernet 3/1/1
```

History

Release version	Command history
08.0.01	This command was introduced.

format disk0

Formats the external USB.

Syntax

format disk0

Modes

User EXEC mode.

Examples

The following example formats the external USB.

```
device# format disk0
Are you sure?(enter 'y' or 'n'): formatting The External USB (disk0) of size 64.2GB
```

History

Release version	Command history
08.0.30	This command was introduced.

gig-default

Configures the Gbps fiber negotiation mode on individual ports overriding the global .

Syntax

gig-default { **neg-full-auto** | **auto-gig** | **neg-off** }

no gig-default { **neg-full-auto** | **auto-gig** | **neg-off** }

Command Default

The globally configured Gbps negotiation mode is the default mode for all Gbps fiber ports.

Parameters

neg-full-auto

Configures the port to first try to perform a handshake with the other port to exchange capability information. If the other port does not respond to the handshake attempt, the port uses the manually configuration (or the defaults if an administrator has not set the information). This is the default.

auto-gig

Configures the port to try to perform a handshake with the other port to exchange capability information.

neg-off

Configures the port to not try to perform a handshake. Instead, the port uses configuration information manually configured by an administrator.

Modes

Interface configuration mode

Usage Guidelines

Gbps negotiation is not supported on ICX 6430, ICX 6450, and ICX 6650 devices.

NOTE
When Gbps negotiation mode is turned off (CLI command **gig-default neg-off**), the device may inadvertently take down both ends of a link. This is a hardware limitation for which there is currently no workaround.

The **no** form of the command resets the configuration to the default, that is to try performing a handshake with other ports to exchange capability information.

Examples

The following example shows how to set the negotiation mode to auto-Gbps for ports 1/1/1 to 1/1/4.

```
device(config)# interface ethernet 1/1/1 to 1/1/4
device(config-mif-1/1/1-1/1/4)# gig-default auto-gig
```

global-filter-strict-security

Re-enables the strict security mode for 802.1X dynamic filter assignment globally.

Syntax

global-filter-strict-security

no global-filter-strict-security

Command Default

Strict security mode is enabled for all 802.1X-enabled interfaces.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command disables strict security mode for 802.1X dynamic filter assignment globally.

Examples

The following example re-enables strict security mode for 802.1X dynamic filter assignment globally.

```
device(config)# dot1x-enable
device(config-dot1x)# global-filter-strict-security
```

The following example disables strict security mode for 802.1X dynamic filter assignment globally.

```
device(config)# dot1x-enable
device(config-dot1x)# no global-filter-strict-security
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

graceful-restart (BGP)

Enables the BGP graceful restart capability.

Syntax

graceful-restart [**purge-time** *seconds* | **restart-time** *seconds* | **stale-routes-time** *seconds*]

no graceful-restart [**purge-time** *seconds* | **restart-time** *seconds* | **stale-routes-time** *seconds*]

Command Default

Graceful restart is enabled globally.

Parameters

purge-time *seconds*

Specifies the maximum period of time, in seconds, for which a restarting device maintains stale routes in the BGP routing table before purging them. Range is from 1 to 3600 seconds. The default value through 600 seconds.

restart-time *seconds*

Specifies the restart time, in seconds, advertised to graceful-restart-capable neighbors. Range is from 1 through 3600 seconds. The default value is 120 seconds.

stale-routes-time *seconds*

Specifies the maximum period of time, in seconds, that a helper device will wait for an End-of-RIB (EOR) marker from a peer. All stale paths are deleted when this time period expires. Range is from 1 through 3600 seconds. The default value is 360 seconds.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to disable the BGP graceful restart capability globally for all BGP neighbors.

Use this command to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. If the graceful restart capability is re-enabled after a BGP session has been established, the neighbor session must be cleared for GR to take effect.

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.

Use this command in BGP configuration mode to disable or re-enable the BGP4 graceful restart capability globally, or to alter the default parameters. Use this command in address-family IPv6 unicast configuration mode to disable or re-enable the BGP4+ graceful restart capability globally or to alter the default parameters.

The **purge-time** parameter is applicable for both restarting and helper devices. The timer starts when a BGP connection is closed. The timer ends when an EOR is received from all nodes, downloaded into BGP and an EOR sent to all neighbors. The configured purge-time timer value is effective only on the configured node.

The **restart-time** parameter is applicable only for helper devices. The timer starts at the time the BGP connection is closed by the remote peer and ends when the Peer connection is established. The configured restart time timer value is effective only on the peer node, and not in the configured node. During negotiation time, the timer value is exchanged.

The **stale-routes-time** parameter is applicable only for helper devices. The timer starts when the peer connection is established once the HA-failover peer node has been established. The timer ends at the time an EOR is received from the peer. The configured stale-time timer value is effective only on the configured node.

Use the **clear ip bgp neighbor** command with the **all** parameter for the changes to the GR parameters to take effect immediately.

Examples

This example disables the BGP4 graceful restart capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# no graceful-restart
```

This example re-enables the BGP4 graceful restart capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# graceful-restart
```

This example disables the BGP4+ graceful restart capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# no graceful-restart
```

This example re-enables the BGP4+ graceful restart capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1000::1 remote-as 2
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 1000::1 activate
device(config-bgp-ipv6u)# graceful-restart
```

This example sets the purge time to 240 seconds at the IPv4 address family configuration level.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-router)# graceful-restart purge-time 240
```

This example sets the restart time to 60 seconds at the IPv4 address family configuration level.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-router)# graceful-restart restart-time 60
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

This example sets the stale-routes time to 180 seconds at the IPv6 address family configuration level.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1000::1 remote-as 2
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 1000::1 activate
device(config-bgp-ipv6u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv6u)# graceful-restart stale-routes-time 180
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

graft-retransmit-timer

Configures the time between the transmission of graft messages sent by a device to cancel a prune state.

Syntax

graft-retransmit-timer *seconds*

no graft-retransmit-timer *seconds*

Command Default

The graft retransmission time is 180 seconds.

Parameters

seconds

Specifies the time in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the default graft retransmission time, 180 seconds.

Messages sent by a device to cancel a prune state are called graft messages. When it receives a graft message, the device responds with a Graft Ack (acknowledge) message. If this Graft Ack message is lost, the device that sent it resends it.

Examples

This example configures a graft retransmission timer to 90 seconds.

```
device(config)# router pim
device(config-pim-router)# graft-retransmit-timer 90
```

group-router-interface

Creates router interfaces for each VLAN in the VLAN group.

Syntax

group-router-interface

no group-router-interface

Command Default

A group router interface is not configured.

Modes

VLAN group configuration mode

Usage Guidelines

The **group-router-interface** command creates router interfaces for each VLAN in the VLAN group by using the VLAN IDs of each of the VLANs as the corresponding virtual interface number. This command enables a VLAN group to use a virtual routing interface group. You can enter this command when you configure the VLAN group for the first time or later, after you have added tagged ports to the VLAN, and so on.

If a VLAN group contains VLAN IDs greater than the maximum virtual interface number allowed, the **group-router-interface** command will be rejected.

The **no** form of the command disables the VLAN group router interface.

Examples

The following example shows how to create a router interface for a VLAN.

```
device(config)# vlan-group 1 vlan 10
device(config-vlan-group-1)# group-router-interface
```

gvrp-base-vlan-id

Configures a VLAN ID as a base VLAN for GVRP.

Syntax

gvrp-base-vlan-id *vlan-id*

no gvrp-base-vlan-id *vlan-id*

Command Default

GVRP uses VLAN 4093 as the base VLAN for the protocol.

Parameters

vlan-id

Configures the new base VLAN. You can specify a VLAN ID from 2 through 4092 or 4095.

Modes

Global configuration mode

Usage Guidelines

All ports that are enabled for GVRP become tagged members of the base VLAN. If you need to use VLAN 4093 for a statically configured VLAN, you can change the GVRP base VLAN ID.

NOTE
If you want to change the GVRP base VLAN ID, you must do so before enabling GVRP.

The **no** form of the command changes the base VLAN to the default VLAN ID of 4093.

Examples

The following example shows how to configure a new base VLAN for GVRP.

```
device(config)# gvrp-base-vlan-id 1001
```

gvrp-enable

Enables the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) and enters GVRP configuration mode.

Syntax

gvrp-enable

no gvrp-enable

Command Default

GVRP is not enabled.

Modes

Global configuration mode

Usage Guidelines

Single STP must be enabled on the device. Brocade implementation of GVRP requires Single STP. If you do not have any statically configured VLANs on the device, you can enable Single STP.

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

Examples

The following example shows how to enable Single STP and then GVRP.

```
device(config)# vlan 1
device(config-vlan-1)# spanning-tree
device(config-vlan-1)# exit
device(config)# spanning-tree single
device(config)# gvrp-enable
device(config-gvrp)#
```

gvrp-max-leaveall-timer

Configures the maximum value for the minimum interval at which GVRP sends Leaveall messages on all GVRP interfaces.

Syntax

gvrp-max-leaveall-timer *time*

no gvrp-max-leaveall-timer *time*

Command Default

The default value is 300,000 milliseconds (ms).

Parameters

time

Specifies the maximum time in milliseconds to which you want to set the Leaveall timer. You can specify from 300,000 to 1,000,000 (one million) milliseconds. The value must be a multiple of 100 ms.

Modes

Global configuration mode

Usage Guidelines

Enter this command before enabling GVRP. Once GVRP is enabled, you cannot change the maximum Leaveall timer value. By default, you can set the Leaveall timer to a value five times the Leave timer - the maximum value allowed by the software (configurable from 300000 ms to 1000000 ms).

This command does not change the default value of the Leaveall timer itself. The command only changes the maximum value to which you can set the Leaveall timer.

The **no** form of the command changes the maximum time value to the default value.

Examples

The following example shows how to set the maximum value for the Leaveall timer.

```
device(config)# gvrp-max-leaveall-timer 1000000
```

hardware-drop-disable

Disables passive multicast route insertion (PMRI).

Syntax

hardware-drop-disable

no hardware-drop-disable

Command Default

PMRI is enabled.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the default and enables PMRI.

To prevent unwanted multicast traffic from being sent to the CPU, PIM routing and PMRI can be used together to ensure that multicast streams are forwarded out only on ports with interested receivers and unwanted traffic is dropped in hardware on Layer 3 switches. To disable this process, use the **hardware-drop-disable** command.

NOTE
Disabling hardware-drop does not immediately take away existing hardware-drop entries, they will go through the normal route aging processing when the traffic stops.

Examples

This example disables PMRI.

```
device(config)#router pim
device(config-pim-router)# hardware-drop-disable
```

hello-interval

Sets the hello-interval in seconds or milliseconds for IPv4 VRRP and IPv6 VRRP.

Syntax

hello-interval { *seconds* | *milliseconds* }

hello-interval msec *milliseconds*

no hello-interval

Command Default

The hello-interval is 1 second.

Parameters

seconds

Specifies the hello-interval in seconds from 1 through 40 seconds for IPv4 VRRP, IPv4 VRRPv3, VRRP-E, and IPv6 VRRP-E. The default is 1 second.

milliseconds

Specifies the hello-interval in seconds from 1 through 84 seconds for IPv4 VRRP, VRRP-E, and IPv6 VRRP-E and 1 through 40 seconds for IPv4 VRRPv3. The default is 1 second.

Modes

VRRP virtual router ID configuration

Usage Guidelines

IPv4 VRRPv2 supports the hello-interval configuration in seconds, while IPv6 VRRP supports this configuration in milliseconds; both use the CLI **hello-interval** . However, IPv4 VRRPv3 supports both the seconds and milliseconds configuration using the **hello-interval** command and the **hello-interval** command with the **msec** option.

Examples

The following example configures the hello-interval on IPv4 VRRPv2 to 20 seconds.

```
device Router1(config)# interface ethernet 1/6
device Router1(config-if-1/6)# ipv4 vrrp vrid 1
device Router1(config-if-1/6-vrid-1)# hello-interval 20
```

The following example configures the hello-interval on IPv4 VRRPv3 to 200 milliseconds.

```
device Router1(config)# interface ethernet 1/6
device Router1(config-if-1/6)# ipv4 vrrp vrid 1
device Router1(config-if-1/6-vrid-1)# hello-interval msec 200
```

History

Release version	Command history
08.0.10	This command was introduced.

hello-timer

Configures the interval at which hello messages are sent out of Protocol Independent Multicast (PIM) interfaces.

Syntax

hello-timer *seconds*

no hello-timer *seconds*

Command Default

The hello interval is 30 seconds.

Parameters

seconds

Specifies the interval in seconds. The range is 10 through 3600 seconds. The default is 30 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the default hello interval, 30 seconds.

Devices use hello messages to inform neighboring devices of their presence.

Examples

This example configures a hello interval of 120 seconds on all ports on a device operating with PIM.

```
device(config)# router pim
device(config-pim-router)# hello-timer 120
```

hitless-failover enable

Enables hitless stacking failover and switchover. The standby controller is allowed to take over the active role without reloading the stack when failover occurs.

Syntax

hitless-failover enable

no hitless-failover enable

Command Default

Hitless stacking failover is enabled. In earlier releases, failover and switchover were disabled by default.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to disable hitless stacking failover. The change takes effect immediately.

The **hitless-failover enable** and **no hitless-failover enable** commands must be executed from the active stack controller.

You must assign a stack mac address to the device using the **stack mac address** command before you can execute the **hitless-failover enable** command.

Examples

The following example enables hitless stacking switchover and failover on the active controller for the stack.

```
device(config)# hitless-failover enable
```

History

Release version	Command history
08.0.00a	This command was introduced.
08.0.20	Hitless failover is enabled by default.

hitless-reload

Performs hitless OS upgrade.

Syntax

hitless-reload [**primary** | **secondary**]

Command Default

Hitless OS upgrade is not enabled.

Parameters

primary

Specifies that the management module will be reloaded with the primary image.

secondary

Specifies that the management module will be reloaded with the secondary image.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on FSX devices only.

If you will be using the **hitless-reload** command to perform the hitless upgrade, you must first copy the software image that supports hitless software upgrade onto the flash memory of the active and standby management modules.

NOTE

The hitless-reload command is accepted only when the running configuration and startup configuration files match. If the configuration file has changed, you must first save the file (**write mem**) before executing a hitless reload.

Examples

The following example shows how to perform a performing a hitless OS upgrade.

```
device# hitless-reload primary
```

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 3 seconds.

Parameters

number

The time interval for the new master to hold the traffic. The time interval ranges from 1 through 84 seconds.

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 1/1/1 to 1/1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# hold-down-interval 4
```

host-max-num

Limits the number of hosts that are authenticated at any one time.

Syntax

host-max-num *number*

no host-max-num *number*

Command Default

There is no limit to the number of hosts that can be authenticated (0).

Parameters

number

Specifies the number of hosts that can be authenticated at any one time. The valid values are from 0 through 8192. The default is 0, that is there is no limit to the number of hosts that can be authenticated.

Modes

Web Authentication configuration mode

Usage Guidelines

The maximum number of hosts that can be authenticated at one time is 8192 or the maximum number of MAC addresses the device supports. When the maximum number of hosts has been reached, the device redirects any new host that has been authenticated successfully to the Maximum Host web page.

The **no** form of the command sets no limit (default).

Examples

The following example limits the number of hosts that can be authenticated at one time to 10.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# host-max-num 10
```

hostname

Configures a system name for a device and saves the information locally in the configuration file for future reference.

Syntax

hostname *string*

no hostname [*string*]

Command Default

The device will have a factory set hostname.

Parameters

string

Configures the system name. The name can be up to 255 alphanumeric characters. The host name should be enclosed in quotation marks if it contains spaces.

Modes

Global configuration mode

Usage Guidelines

When you configure a system name, the name replaces the default system name in the CLI command prompt.

The **no** form of the command removes the configured hostname..

Examples

The following example shows how to configure a system name.

```
device(config)# hostname zappa
zappa(config)#
```

ignore-temp-shutdown

Prevents shutdown of ICX 7450 and ICX 7750 devices when the device reaches the threshold shutdown temperature. At a time, either the global battleshort mode or unit specific battleshort mode is enabled but not both.

Syntax

ignore-temp-shutdown

no ignore-temp-shutdown

Command Default

By default, the function is disabled.

Modes

Global configuration mode and unit level configuration mode

Usage Guidelines

This command is applicable only on ICX7450 and ICX7750 devices. This command can be executed at a global level and at a unit level. If the command is enabled or disabled at global level, it applies to all the units which are part of the stack. If the command is enabled or disabled at a unit level, it applies only to that unit alone in the stack. To execute this command at a unit level, specify the unit ID at the configuration mode. The "no" form of the command disables the battleshort mode at global level and at unit level.

Examples

```
device(config)# ignore-temp-shutdown
device(config)#
device(config)# no ignore-temp-shutdown
device(config)#

device(config-unit-1)# ignore-temp-shutdown
device(config-unit-1)#
device(config-unit-1)# no ignore-temp-shutdown
device(config-unit-1)#
```

History

Release version	Command history
8.0.30j	This command is newly introduced.

import-users

Imports a text file of user records from a TFTP server to the device.

Syntax

import-users tftp *ip-address* **filename** *name*

Parameters

tftp *ip-address*

Specifies the IP address of the TFTP server from which the file must be imported.

filename *name*

Specifies the name of the file to import from the TFTP server.

Modes

Local user database configuration mode

Usage Guidelines

Before importing the file, make sure it adheres to the ASCII text format. The text file to be imported must be in the following ASCII format.

```
[delete-all]
[no] username
username1
password
password1
cr
[no] username
username2
password
password2
cr
...
```

The **delete-all** command entry in the text file indicates that the user records in the text file will replace the user records in the specified local user database on the switch. If the **delete-all** entry is not present, the new user records will be added to the specified local user database on the switch. The **delete-all** command entry is optional. If present, it must appear on the first line, before the first user record in the text file. If you want to delete a user entry from the specified local user database on the switch, use the **no username** command entry in the text file. User records that already exist in the local user database will be updated with the information in the text file when it is uploaded to the switch. For username1, username2, and so on, enter up to 31 ASCII characters.

Examples

The following example imports a text file of user records from a TFTP server.

```
device(config)# local-userdb userdb1
device(config-localuserdb-userdb1)# import-users tftp 192.168.1.1 filename userdb1
```

inactivity-timer

Configures the time a forwarding entry can remain unused before the device deletes it.

Syntax

inactivity-timer *seconds*

no inactivity-timer *seconds*

Command Default

The default inactive time is 180 seconds.

Parameters

seconds

Specifies the time in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the default inactive time, 180 seconds.

A device deletes a forwarding entry if the entry is not used to send multicast packets. The Protocol Independent Multicast (PIM) inactivity timer defines how long a forwarding entry can remain unused before the device deletes it.

Examples

This example configures an inactive time to 90 seconds.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# inactivity-timer 90
```

include-port

Adds ports to the VSRP.

Syntax

include-port ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]

no include-port ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]

Command Default

By default, all the ports on which you configure a VRID are interfaces for the VRID.

Parameters

ethernet *stackid/slot/port*

Adds the Ethernet interface to the VRID.

to *stackid/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 1/1/1 to 1/1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# no include-port ethernet 1/1/2
```

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 1/1/1 to 1/1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# initial-ttl 5
```

inline power

Configures inline power on Power over Ethernet (PoE) ports in interface configuration mode and link aggregation group (LAG) secondary ports in global configuration mode.

Syntax

inline power ethernet *interface* [**decouple-datalink**] [**power-by-class** *power-class*] [**power-limit** *power-limit*] [**priority** *priority -value*]

no inline power ethernet *interface* [**decouple-datalink**] [**power-by-class** *power-class*] [**power-limit** *power-limit*] [**priority** *priority -value*]

NOTE

The **ethernet***interface* pair of parameters is required only if you want to configure inline power on secondary ports (you must use global configuration mode to do this).

Parameters

ethernet

Specifies an ethernet interface. You can configure the **ethernet** keyword only in global configuration mode.

interface

Specifies the number of the ethernet interface. This is used only with the **ethernet** keyword.

decouple-datalink

Specifies decoupling of datalink and PoE so that datalink state changes do not affect the PoE state. You can configure the **decouple-datalink** keyword in global and interface configuration modes.

power-by-class

Specifies the power limit based on class value. The range is 0-4. The default is 0.

power-limit

Specifies the power limit based on actual power value in mW. The range is 1000-15400|30000mW. The default is 15400|30000mW. For PoH ports, the range is 1000-95000mW, and the default is 95000mW. The power-limit value is rounded to the nearest multiple of 5 on PoH ports.

priority

Specifies the priority for power management. The range is 1 (highest) to 3 (lowest). The default is 3.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

You cannot configure inline power on PoE LAG ports in interface configuration mode because the interface-level configuration is not available in the CLI for LAG secondary ports. The **inline power ethernet** command enables you to configure inline power on secondary ports in global configuration mode.

The **decouple-datalink** keyword was introduced in Release 08.0.01 to support the inline-power functionality. The decouple-datalink functionality is not supported in releases earlier than Release 08.0.01.



WARNING
If you want to keep decoupling in place on a PoE port when you configure the **inline power ethernet** command to change its other parameters, (for example, priority) you must also configure the **decouple-datalink** keyword.



WARNING
If you downgrade to a release earlier than 08.0.01, you cannot use **inline power** commands that have the **decouple-datalink** keyword. Any **inline power** commands in the startup config will not be effective.

Examples

Examples

The following example configures inline power on LAG ports.

```
Device(config)# lag "mylag" static id 5
Device(config-lag-mylag)# ports ethernet 1/1/1 to 1/1/4
Device(config-lag-mylag)# primary-port 1/1/1
Device(config-lag-mylag)# deploy
LAG mylag deployed successfully!
Device(config)#inline power ethernet 1/1/1 power-by-class 3
Device(config)#inline power ethernet 1/1/2
Device(config)#inline power ethernet 1/1/3 priority 2
Device(config)#inline power ethernet 1/1/4 power-limit 12000
```

Examples

The following example decouples the behavior of the PoE and the datalink operations for PoE LAG ports. After the optional **decouple-datalink** keyword in the **inline power ethernet** command is entered, the datalink operational behavior on a PoE port does not affect the power state of the powered device (PD) that is connecting to the port.

```
Device(config)#inline power ethernet 1/1/1 decouple-datalink power-by-class 3
Device(config)#inline power ethernet 1/1/2 decouple-datalink
Device(config)#inline power ethernet 1/1/3 decouple-datalink priority 2
Device(config)#inline power ethernet 1/1/4 decouple-datalink power-limit 12000
Device(config)# lag "mylag" static id 5
Device(config-lag-mylag)# ports ethernet 1/1/1 to 1/1/4
Device(config-lag-mylag)# primary-port 1/1/1
Device(config-lag-mylag)# deploy
LAG mylag deployed successfully!
```

Examples

The following example decouples the behavior of the PoE and the datalink operations for regular PoE ports. After the optional **decouple-datalink** keyword in the **inline power** command is entered, the datalink operational behavior on a PoE port does not affect the power state of the powered device (PD) that is connecting to the port.

```
Device(config)# interface ethernet 1/1/1
Device(config-if-e1000-1/1/1)# inline power decouple-datalink power-by-class 3
Device(config-if-e1000-1/1/1)# interface ethernet 1/1/2
Device(config-if-e1000-1/1/2)# inline power decouple-datalink
Device(config-if-e1000-1/1/2)# interface ethernet 1/1/3
Device(config-if-e1000-1/1/3)# inline power decouple-datalink priority 2
Device(config-if-e1000-1/1/3)# interface ethernet 1/1/4
Device(config-if-e1000-1/1/4)# inline power decouple-datalink power-limit 12000
```

History

Release	Command History
08.0.01	This command was modified to run in global configuration mode using the **ethernet** keyword. The **decouple-datalink** keyword was also introduced.
08.0.20	This command was modified to allow requisite PoH power limits.

inline power adjust class

Use these commands when powered devices (PDs) are entering an overload state as a result of faulty PDs power requests.

Syntax

inline power adjust classr *class* { **delta** *milliwatts* | **minimum** *milliwatts* }

no inline power adjust classr *class* { **delta** *milliwatts* | **minimum** *milliwatts* }

Parameters

class
: The detected PD class for which this configuration is applied to. Values ramge from 0 through 4.

delta
: Tthe amount of extra power allocated above the LLDP/CDP requested power.

milliwatts
: The additional allocated power measured in milliwatts.

minimum
: The minimum power that must be allocated, even if the PD LLDP/CDP requested power is lower than the configuration.

Modes

Global configuration mode

Usage Guidelines

These configurations should be used only when ports are entering an overload condition because of faulty PDs that are requesting lower power through LLDP/CDP messages and then consuming higher than the requested power.

The delta option assures the power allocation is equal to LLDP/CDP requested power plus delta power that is configured for that PD class.

The minimum option assures that the power allocation is equal to the maximum of LLDP/CDP power requested and the minimum power configured for that PD class.

Given a configuration of **inline power adjust class** 1 **delta** 800. If a class 1 PD is connected and is requesting power of 2600 milliWatts through LLDP/CDP, then the total allocation from the switch would be 3200 milliWatts. But if a class 2 PD is connected then there won't be any extra power allocation. If you want the extra power allocation for a class 2 PD, the configuration would be **inline power adjust class** 2 **delta** 800.

Examples

Set the detected PD class to 1 and allocate 800 milliwatts of extra power for the class.

```
device(config)# inline power adjust class 1 delta  800
```

Set the detected PD class to 1 and allocate minimum power (in milliwatts) regardless of the LLDP/CDP requested power level.

```
device(config)# inline power adjust class 1 minimum  3200
```

History

Release	Command History
8.0.30f	This command was introduced.

inline power budget

Sets the power budget for a PoE interface module.

Syntax

inline power budget budget *num* **module** *slot*

Command Default

Each PoE and PoE+ interface module has a maximum power budget of 65535 watts.

Parameters

num

Specifies the number of milliwatts to allocate to the module. The value can range from 0 to 65535000.

module *slot*

Specifies where the PoE or PoE+ module resides in the chassis.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on FSX devices.

Examples

The following example shows how to change the power allocation.

```
device(config)# inline power budget 150000 module 7
```

inline power install-firmware

Installs Power over Ethernet (PoE) firmware.

Syntax

inline power install-firmware { **all** | **stack-unit** *unit-number* } **tftp** *ip-address file-name*

Parameters

all

Installs Firmware on all PoE units of the system. This option is supported only on ICX 7450 and ICX 7250.

stack-unit *unit-number*

Specifies the unit ID of the stack. If the switch is not a part of the stack, the unit number is the default value. The default stack-unit value is 1.

tftp *ip-address*

Specifies the IP address of the TFTP server.

file-name

Specifies the name of the file, including its path name.

Modes

Privileged EXEC mode

Usage Guidelines

PoE Firmware download can be initiated on one stack unit at a time on the FSX and FCX devices.

On ICX 7250 and ICX 7450 devices, PoE Firmware download can be initiated on one stack unit at a time or on all PoE units or multiple stacks simultaneously.

Examples

The following example installs PoE firmware.

```
device# inline power install-firmware stack-unit 1 tftp 10.120.54.161 icx74xx_poh_01.8.8.b001.fw
```

The following example installs PoE firmware on all PoE units.

```
device# inline power install-firmware all tftp 10.120.54.161 icx74xx_poh_01.8.8.b001.fw
```

History

Release version	Command history
08.0.30p	The command was modified to add the **all** keyword.

inline power install-firmware scp

Upgrades the PoE firmware of a Brocade SX module or FastIron stacking device by downloading a firmware file from an SCP server.

Syntax

inline power install-firmware { **all** | **stack-unit** *unit-id* | **module** *module-id* } **scp** { *ipv4-address-* | *ipv4-hostname-* | **ipv6** { *ipv6-address-* | *ipv6-hostname-* } **outgoing-interface** { **ethernet** *stackid/slot/port* | **ve** *ve-number* } } [**public-key** { **dsa** | **rsa** }] [*remote-port*] *remote-filename*

Parameters

all

Installs Firmware on all PoE units of the system. This option is supported only on ICX 7450 and ICX 7250.

stack-unit *unit-id*

Specifies the unit ID of the FastIron device in the stack to copy the PoE firmware. You must specify the stack unit when you configure the **inline power install-firmware** command to upgrade PoE firmware on a stacking device.

module *module-id*

Specifies the module ID of the Brocade SX device to copy the PoE firmware. You must specify the module when you configure the **inline power install-firmware** command to upgrade PoE firmware on a Brocade SX device.

ipv4-address-

Specifies the IPV4 address of the SCP server, using 8-bit values in dotted decimal notation.

ipv4-hostname-

Specifies the IP hostname of the SCP server.

ipv6

Specifies the IPV6 address method for SCP file transfer.

ipv6-address-prefix/prefix-length

Specifies the IPV6 address of the SCP server. You must specify this address in hexadecimal using 16-bit values between colons, as documented in RFC 2373.

ipv6-hostname-

Specifies the IPv6 hostname of the SCP server.

outgoing-interface

Specifies the interface to be used to reach the remote host.

ethernet *stackid/slot/port*

Configures an Ethernet interface as the outgoing interface.

ve *ve-number*

Configures a virtual interface (VE) as the outgoing interface.

public-key

Specifies the type of public key authentication to use for the connection, either digital signature algorithm (DSA) or Rivest, Shamir, and Adelman (RSA) . If you do not configure this parameter, the default authentication type is password.

dsa

Specifies DSA as the public key authentication.

rsa
Specifies RSA as the public key authentication.

remote-port
Specifies the remote port number for the TCP connection.

remote-filename
Specifies the name of the file in the SCP server that is be transferred. You can specify up to 127 characters for the filename.

Modes

Privileged EXEC mode

Usage Guidelines

You are prompted for username and password when you configure this command.

If you do not configure the type of public key authentication, the default authentication type is password.

You must specify the stack unit and module when you configure the **inline power install-firmware** command to upgrade PoE firmware on a stacking device.

PoE Firmware download can be initiated on one stack unit at a time on the FSX and FCX devices.

On ICX 7250 and ICX 7450 devices, PoE Firmware download can be initiated on one stack unit at a time or on all PoE units or multiple stacks simultaneously.

Examples

This example upgrades the PoE firmware of a FastIron device by downloading a firmware file from an SCP server:

```
Device#inline power install-firmware stack-unit 2 scp 2.2.2.2 icx74xx_poh_01.8.8.b001.fw
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.30p	The command was modified to add the **all** keyword.

inline power interface-mode-2pair-pse

Corrects a condition where some non-standard powered devices (PD) are undetected on PoH ports due to difference in allowed capacitance between a 2-pair port and a 4-pair port.

Syntax

inline power interface-mode-2pair-pse

Modes

Configure interface port extender.

Usage Guidelines

This command is for the Brocade ICX 7450 24P and ICX 7450 48P platforms.

Before this command is executed the user may see the following behavior:

```
SPX(config)# interface ethernet 17/1/8
SPX(config-if-pe-e1000-17/1/8)# enable
SYSLOG: <14> Sep 27 17:32:49 SPX PORT: 17/1/8 enabled by un-authenticated user
from console session.
SYSLOG: <14> Sep 27 17:32:49 SPX System: PoE: Allocated power of 95000 mwatts
on port 17/1/8.
SYSLOG: <14> Sep 27 17:32:56 SPX System: PoE: Released complete power of 95000
mwatts on port 17/1/8.
SPX(config-if-pe-e1000-17/1/8)# show inline power 17/1/8

 Port   Admin   Oper    ---Power(mWatts)---  PD Type  PD Class  Pri  Fault/
        State   State   Consumed  Allocated                        Error
-----------------------------------------------------------------------------
 17/1/8 On      Off            0          0  n/a      n/a         3  n/a
```

Where the Operating State is listed as Off, there is no power consumed or allocated, and the PD is not recognized..

Examples

To correct this problem:

```
SPX# configure terminal
SPX(config)# interface ethernet 17/1/8
SPX(config-if-pe-e1000-17/1/8)# inline power interface-mode-2pair-pse
SYSLOG: <14> Sep 27 17:34:52 SPX System: PoE: Allocated power of 7000 mwatts on
port 17/1/8. PoE: Power enabled on port 17/1/8.
SYSLOG: <14> Sep 27 17:34:52 SPX System: PoE: Power enabled on port 17/1/8.
SYSLOG: <14> Sep 27 17:34:52 SPX System: Interface ethernet 17/1/8, state up
SPX(config-if-pe-e1000-17/1/8)# show running-config interface ethernet 17/1/8
interface ethernet 17/1/8
 spanning-tree root-protect
 spanning-tree 802-1w admin-edge-port
 inline power
 inline power interface-mode-2pair-pse
 stp-bpdu-guard
 trust dscp
 port security
 enable
!
SPX(config-if-pe-e1000-17/1/8)# show inline power 17/1/8

 Port   Admin   Oper    ---Power(mWatts)---  PD Type  PD Class  Pri  Fault/
        State   State   Consumed  Allocated                       Error
-----------------------------------------------------------------------
 17/1/8 On      On          2700       7000  Legacy   Class 2     3  n/a
```

History

Release version	Command history
08.0.30	This command was introduced.

inline power non-pd-detection enable

Enables detection for non powered endpoints or devices (non-PD).

Syntax

inline power non-pd-detection enable

no inline power non-pd-detection enable

Command Default

By default, the non-PD detection logic is disabled.

Modes

Global configuration mode.

Usage Guidelines

Once this feature is enabled, only new devices connected to the Power over Ethernet (PoE) ports are detected. The existing non-PDs are not detected.

A multiport PD must be connected to a single unit and must have a LAG defined for the ports.

To detect existing non-PDs, you must save the configuration and reload the device or follow the below order of configuration:

1. Configure the LAG for multiport PDs.
2. Enable non-PD detection mode.
3. Configure inline power on interfaces.

The **no** form of the command disables the non-PD detection. However, the existing non-PD state declarations on the ports are not cleared. The state declarations on the ports clear when they are disconnected from the non-PDs or when you save the configuration and reload the device.

Either reload after disabling the mode or disable and then enable inline power on ports that are in a non-PD state.

When a port has detected a non-PD, it generates the syslog message:

```
PoE: Power disabled on port 1/1/21 because of detection of non-PD.
PD detection will be disabled on port.
```

When a port loses a non-PD (cable disconnected, etc.), it generates the syslog message:

```
PoE: Port 1/1/21 lost non-PD, so enabling PD detection.
```

Examples

The following example enables non-PD detection.

```
device# configure terminal
device(config)# inline power non-pd-detection enable
Warning: Enabling or disabling non-PD detection requires reload or
disable/enable of ports with existing non-PDs.
Warning: Enabling this configuration also has following limitation:
All ports of a multi-port PD must be connected to one unit only so
that a LAG configured does not span more than a single unit.
device(config)# write memory
device(config)# exit
device# reload
```

History

Release version	Command history
08.0.30f	This command was introduced.

interface ethernet

Enters interface configuration mode for the specified Ethernet interface.

Syntax

interface ethernet *stackid/slot/port* [[**ethernet** *stackid/slot/port*]... | **to** *stackid/slot/port*]

no interface ethernet *stackid/slot/port* [[**ethernet** *stackid/slot/port.*]... | **to** *stackid/slot/port*]

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet interface.

to *stackid/slot/port*

Specifies a range of Ethernet interfaces.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of the command exits from the interface configuration mode.

Examples

The following example shows how to enter interface configuration mode.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# interface ethernet 1/1/2
```

The following example shows how to move to one interface mode to another.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# interface ethernet 1/1/2
device(config-if-e1000-1/1/2)#
```

interface group-ve

Associates the virtual interface routing group with a VLAN group.

Syntax

interface group-ve *num*

no interface group-ve *num*

Command Default

A virtual routing interface group is not associated with a VLAN group.

Parameters

num

Specifies the VLAN group ID with which you want to associate the virtual routing interface group.

Modes

Global configuration mode

Usage Guidelines

The VLAN group must already be configured and enabled to use a virtual routing interface group. The software automatically associates the virtual routing interface group with the VLAN group that has the same ID. You can associate a virtual routing interface group only with the VLAN group that has the same ID.

When you configure a virtual routing interface group, all members of the group have the same IP subnet address.

NOTE
Configuring a virtual interface routing group is not supported with IPv6. It is also not supported on FCX devices with ACLs. Configuring a virtual interface routing group is supported only with the OSPF, VRRPv2, and VRRP-Ev2 protocols.

The **no** form of the command removes the virtual routing interface group from a VLAN group.

Examples

The following example shows how to associate the virtual routing interface group with a VLAN group.

```
device(config)# vlan-group 1
device(config-vlan-group-1)# group-router-interface
device(config-vlan-group-1)# exit
device(config)# interface group-ve 1
```

interface tunnel

Configures a tunnel interface.

Syntax

interface tunnel *tunnel-number*

no interface tunnel *tunnel-number*

Command Default

No tunnel interface is configured.

Parameters

tunnel-number

Specifies the tunnel number.

Modes

Global configuration mode

Usage Guidelines

Use the **no interface tunnel** command to remove the tunnel interface.

Examples

This example creates a tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 2
device(config-tnif-2)#
```

Related Commands

tunnel destination, tunnel mode gre ip, tunnel source

ip access-group

Applies ACL to ports.

Syntax

ip access-group { *acl-num* | *acl-name* } { **in** [**ethernet** *stack/slot/port* [**to** *stack/slot/port* | [**ethernet** *stack/slot/port* **to** *stack/slot/port* | **ethernet** *stack/slot/port*] ...]] | **out** }

no ip access-group { *acl-num* | *acl-name* } { **in** [**ethernet** *stack/slot/port* [**to** *stack/slot/port* | [**ethernet** *stack/slot/port* **to** *stack/slot/port* | **ethernet** *stack/slot/port*] ...]] | **out** }

ip access-group frag deny

no ip access-group frag deny

Command Default

ACLs are not applied to ports.

Parameters

acl-num
Specifies the access list number. You can specify from 1 through 99 for standard ACLs and from 100 through 199 for extended ACLs.

acl-name
Specifies the access list name. You can specify a string of up to 256 alphanumeric characters.

in
Configures the ACL to be applied on inbound traffic on the port.

ethernet *stack/slot/port*
Specifies the Ethernet interface from which the packets are coming.

to *stack/slot/port*
Specifies the range of Ethernet interfaces from which the packet are coming.

out
Configures the ACL to be applied to the outbound traffic on the port.

frag deny
Denies all IP fragments on the port.

Modes

Interface configuration mode

Usage Guidelines

You can use blank spaces in the ACL name if you enclose the name in quotation marks (for example, "ACL for Net1").

You can apply an IPv4 ACL to a virtual routing interface. The virtual interface is used for routing between VLANs and contains all the ports within the VLAN. The IPv4 ACL applies to all the ports on the virtual routing interface. You also can specify a subset of ports within the VLAN containing a specified virtual interface when assigning an ACL to that virtual interface.

The **no** form of the command removes applied ACL from a port.

Examples

The following example shows how to apply an ACL to a port.

```
device(config)# ip access-list standard Net1
device(config-std-nACL)# deny host 10.157.22.26 log
device(config-std-nACL)# deny 10.157.29.12 log
device(config-std-nACL)# deny host IPHost1 log
device(config-std-nACL)# permit any
device(config-std-nACL)# exit
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ip access-group Net1 in
```

The following example shows how to apply ACL to a subset of ports within a virtual interface.

```
device(config)# enable acl-per-port-per-vlan
...
device(config)# vlan 10 name IP-subnet-vlan
device(config-vlan-10)# untag ethernet 1/1/1 to 2/1/10
device(config-vlan-10)# router-interface ve 1
device(config-vlan-10)# exit
device(config)# access-list 1 deny host 10.157.22.26 log
device(config)# access-list 1 deny 10.157.29.12 log
device(config)# access-list 1 deny host IPHost1 log
device(config)# access-list 1 permit any
device(config)# interface ve 1/1/1
device(config-vif-1/1/1)# ip access-group 1 in ethernet 1/1/1 ethernet 1/1/3 ethernet 2/1/2 to 2/1/4
```

ip access-list

Configures a standard or extended access list.

Syntax

ip access-list { **standard** | **extended** } { *acl-num* | *acl-name* }

no ip access-list { **standard** | **extended** } { *acl-num* | *acl-name* }

Command Default

The IP access list is not configured.

Parameters

standard
Configures a standard access list.

extended
Configures an extended access list.

acl-num
Specifies the ACL number for a standard or extended access list. The value can be from 1 through 99 for standard ACLs and from 100 through 199 for extended ACLs.

acl-name
Specifies the ACL name for a standard or extended access list. You can specify a string of up to 256 alphanumeric characters.

Modes

Global configuration mode

Usage Guidelines

You can use blank spaces in the ACL name if you enclose the name in quotation marks (for example, "ACL for Net1").

Once you configure the ACL, you must use the **permit** or **deny** commands to configure the rules for the ACL.

The **no** form of the command removes the configured access list.

Examples

The following example configures a standard access list.

```
device(config)# ip access-list standard acl1
device(config-std-nacl)#
```

The following example configures an extended access list.

```
device(config)# ip access-list extended 125
device(config-ext-nacl)#
```

ip add-host-route-first

Enables to establish the TCP connection as a part of first TCP handshake itself, when an TCP connection establishment packet is routed to a destination interface for which ARP is not resolved.

Syntax

ip add-host-route-first

no ip add-host-route-first

Command Default

TCP connections are not established as a part of the first TCP handshake, when an TCP connection establishment packet is routed to a destination interface for which ARP is not resolved.

Modes

Global configuration mode

Usage Guidelines

Use this command when an TCP connection establishment packet is routed to a destination interface for which ARP is not resolved. This helps to establish the connection as a part of first TCP handshake itself.

The **no** form of the command removes the configuration which enables the establishment of TCP connection as a part of first TCP handshake.

Examples

The following example establishes the TCP connection as a part of first TCP handshake itself.

```
device(config)# ip add-host-route-first
```

History

Release version	Command history
08.0.30e	This command was introduced.

ip address

Assigns IP address to an interface.

Syntax

ip address *ip-addr*

no ip address { *ip-addr* | * }

Parameters

ip-addr

Configures the IP address. Specify the IP address in the format A.B.C.D with mask address or A.B.C.D/L.

*

Deletes all IP address.

Modes

Interface configuration mode

Usage Guidelines

Use * to delete all the IP addresses.

The **no** form of the command removes the IP address from the interface.

Examples

The following example shows how to assign an IP address.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ip address 192.168.10.1 255.255.255.0
```

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 1/1/1 to 1/1/8
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# ip-address 10.10.10.1
```

ip arp inspection validate

Enables validation of the ARP packet destination MAC, ARP Packet IP, and source MAC addresses.

Syntax

ip arp inspection validate [**dst-mac** | **ip** | **src-mac**]

Command Default

IP ARP packet destination address validation is disabled.

Parameters

dst-mac

Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip

Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

src-mac

Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

Modes

Global configuration mode

Usage Guidelines

You can enable validation of ARP packet destination addresses for a single destination address or for all destination addresses.

You must execute the command once for each type of ARP packet destination address you want to validate.

Examples

The following example enables validation of the MAC, ARP Packet IP, and source MAC ARP packet destination addresses.

```
device(config)# configure terminal
device(config)# ip arp inspection validate dst-mac
device(config)# ip arp inspection validate src-mac
device(config)# ip arp inspection validate ip
```

History

Release version	Command history
08.0.10a	This command was introduced.

ip arp inspection syslog disable

Disables the syslog messages for Dynamic ARP Inspection.

Syntax

ip arp inspection syslog disable

no ip arp inspection syslog disable

Command Default

Syslog messages are enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command re-enables syslog messages for Dynamic ARP Inspection.

Examples

The following example disables the syslog messages for dynamic ARP inspection.

```
device(config)# ip arp inspection syslog disable
```

History

Release version	Command history
08.0.30b	This command was introduced.

ip arp inspection vlan

Enables dynamic ARP inspection on a VLAN.

Syntax

ip arp inspection vlan *vlan-number*

no ip arp inspection vlan *vlan-number*

Command Default

Dynamic ARP inspection is disabled by default.

Parameters

vlan-number

Specifies the VLAN number.

Modes

Global configuration mode

Usage Guidelines

The no form of this command disables this functionality.

Examples

The following example shows enabling IP ARP inspection on VLAN 2.

```
device(config)# ip arp inspection vlan 2
```

ip bootp-gateway

Changes the IP address used for stamping BootP or DHCP requests received on the interface.

Syntax

ip bootp-gateway *ip-address*

Parameters

ip-address

Specifies the IP address used to stamp requests received on the interface.

Modes

Interface configuration mode

Usage Guidelines

The BootP or DHCP stamp address is an interface parameter. Use this command to change the parameter on the interface that is connected to the BootP/DHCP client.

In the example given below the command changes the CLI to the configuration level for port 1/1, then changes the BootP or DHCP stamp address for requests received on port 1/1 to 10.157.22.26. The Layer 3 switch will place this IP address in the Gateway Address field of BootP or DHCP requests that the Layer 3 switch receives on port 1/1 and forwards to the BootP or DHCP server.

Examples

The following command changes the IP address used for stamping BootP or DHCP requests received on interface 1/1/1.

```
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# ip bootp-gateway 10.157.22.26
```

ip bootp-use-intf-ip

Configures a Dynamic Host Configuration Protocol (DHCP) relay agent to set the source IP address of a DHCP-client packet with the IP address of the interface in which the DHCP-client packet is received.

Syntax

ip bootp-use-intf-ip

no ip bootp-use-intf-ip

Command Default

The DHCP relay agent sets the source IP address of a DHCP-client packet with the IP address of the outgoing interface to the DHCP server.

Modes

Global configuration mode

Usage Guidelines

You can configure ACLs on a DHCP server to permit or block access to the DHCP server from particular subnets or networks. You can then use this command on the DHCP relay agent to reveal the source subnet or network of a DHCP packet to the DHCP server, which enables the DHCP server to process or discard the DHCP traffic according to the configured ACLs.

no

Examples

The following example configures a FastIron DHCP relay agent so that it sets the source IP address of a DHCP-client packet with the IP address of the interface on which the DHCP-client packet is received.

```
device(config)# ip bootp-use-intf-ip
```

ip dhcp-client auto-update enable

Enables the DHCP auto-update functionality.

Syntax

ip dhcp-client auto-update enable

no ip dhcp-client auto-update enable

Command Default

DHCP client auto-update is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables DHCP auto-update.

Examples

The following example re-enables auto-update.

```
device(config)# ip dhcp-client auto-update enable
```

ip dhcp-client enable

Enables DHCP client auto-update.

Syntax

ip dhcp-client enable

no ip dhcp-client enable

Modes

Global configuration mode.

Interface configuration mode.

Usage Guidelines

The **no** form of the command disables the DHCP client.

You can enable this command on a switch in global configuration mode. On routers, you can enable this command in interface configuration mode.

Examples

The following example enables the DHCP client on a switch.

```
device(config)# ip dhcp-client enable
```

The following example enables the DHCP client on a router.

```
device(config-if-e1000-0/1/1)# ip dhcp-client enable
```

ip dhcp-client continuous-mode max-duration

Limits the level of IPv4 address acquisition attempts globally on a DHCP client.

Syntax

ip dhcp-client continuous-mode max-duration *interval*

no dhcp-client continuous-mode max-duration *interval*

Command Default

The default time is one hour.

Parameters

interval

Specifies the interval value for the DHCP client to limit or stop the address acquisition feature in hours. The minimum time is 1 hour and the maximum time is 65535 hours.

Modes

Global configuration mode

Usage Guidelines

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

Address acquisition stops once it reaches the configured maximum duration.

Examples

The following example sets the maximum duration interval to two hours.

```
device(config)# ip dhcp-client continuous-mode max-duration 2
```

History

Release version	Command history
08.0.30	This command was introduced.

ip dhcp-client discover-interval

Specifies the discover interval value for the DHCP client to acquire IPv4 addresses.

Syntax

ip dhcp-client discover-interval *interval*

no ip dhcp-client discover-interval *interval*

Command Default

The default interval is 10 minutes.

Parameters

interval

Specifies the interval value for the DHCP client to acquire IPv4 addresses, in minutes. The minimum is 5 minutes, while the maximum time is 60 minutes.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of this command disables the functionality.

Use this command to configure the discover-interval value. The DHCP client starts sending discover messages based on the interval value you configure on the device.

Examples

The following example configures the client to send discover messages at intervals of every 20 minutes. This global configuration mode is applicable only for a switch.

```
device(config)# ip dhcp-client discover-interval 20
```

The following example configures the client to send discover messages at intervals of every 20 minutes. The interface configuration mode is applicable only for a router.

```
device(config-if-e1000-0/1/1)# ip dhcp-client discover-interval 20
```

History

Release version	Command history
08.0.30	This command was introduced.

ip dhcp-server arp-ping-timeout

Sets the ARP-ping timeout value.

Syntax

ip dhcp-server arp-ping-timeout *number*

no ip dhcp-server arp-ping-timeout *number*

Command Default

ARP-ping timeout is not enabled.

Parameters

number

The number of seconds to wait for a response to an ARP-ping packet. The minimum setting is 5 seconds and the maximum is 30 seconds.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command disables the ARP ping timeout. If there is no response to the ARP-ping packet within a set amount of time (set in seconds), the server deletes the client from the lease-binding database.

NOTE
Do not alter the default value unless it is necessary. Increasing the value of this timer may increase the time to get console access after a reboot.

Examples

The following example sets the ARP-ping timeout to 25 seconds.

```
device# ip dhcp-server arp-ping-timeout 25
```

ip dhcp-server enable

Enables the DHCP server.

Syntax

ip dhcp-server enable

no ip dhcp-server enable

Command Default

The DHCP server is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables the DHCP server.

Examples

The following example enables the DHCP server.

```
device(config)# ip dhcp-server enable
```

ip dhcp-server mgmt

Enables or disables the DHCP server on the management port.

Syntax

ip dhcp-server mgmt

no ip dhcp-server mgmt

Command Default

DHCP server management is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the DHCP server on the management port.

When disabled, DHCP client requests that are received on the management port are discarded.

Examples

The following example enables the DHCP server on the management port.

```
device(config)# ip dhcp-server mgmt
```

The following example disables the DHCP server on the management port.

```
device(config)# no ip dhcp-server mgmt
```

ip dhcp-server server-identifier

Specifies the IP address of the selected DHCP server.

Syntax

ip dhcp-server server-identifier *ip-address*

Parameters

ip-address

Specifies the IP address of the DHCP server.

Modes

Global configuration mode

Examples

The following example shows assigning an IP address to the selected DHCP server.

```
device(config)# ip dhcp-server-identifier 10.1.1.144
```

ip dhcp-server pool

Creates a DHCP server address pool.

Syntax

ip dhcp-server pool *name*

no ip dhcp-server pool *name*

Parameters

name

The name of the address pool.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of this command disables the address pool. Use this command to switch to pool configuration mode (config-dhcp-name# prompt) and create an address pool.

Examples

The following example creates a DHCP address pool.

```
device(config)# ip dhcp-server pool cabo
```

ip dhcp-server relay-agent-echo enable

Activates the DHCP option 82.

Syntax

ip dhcp-server relay-agent-echo enable

Command Default

The DHCP option 82 functionality is not enabled by default.

Modes

Global configuration mode

Usage Guidelines

This command enables the DHCP server to echo the entire contents of the relay agent information option in all replies.

Examples

The following example enables the DHCP server relay agent.

```
device(config)# ip dhcp-server relay-agent-echo enable
```

ip dhcp snooping vlan

Enables DHCP snooping on a VLAN.

Syntax

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping vlan *vlan-id*

Command Default

DHCP snooping is disabled by default.

Parameters

vlan-id

Specifies the ID of a configured client or DHCP server VLAN.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command disables DHCP snooping on the specified VLAN.

When DHCP snooping is enabled on a VLAN, DHCP packets are inspected. DHCP snooping must be enabled on the client and the DHCP server VLANs.

Examples

The following example enables DHCP snooping on VLAN 2.

```
device(config)# ip dhcp snooping vlan 2
```

ip dhcp relay information policy

Configures the DHCP relay information policy.

Syntax

ip dhcp relay information policy [**drop** | **keep** | **replace**]

Command Default

The device replaces the information with its own relay agent information.

Parameters

drop

Configures the device to discard messages containing relay agent information.

keep

Configures the device to keep the existing relay agent information.

replace

Configures the device to overwrite the relay agent information with the information in the Brocade configuration.

Modes

Global configuration mode.

Usage Guidelines

When the Brocade device receives a DHCP message that contains relay agent information, if desired, you can configure the device to keep the information instead of replacing it, or to drop (discard) messages that contain relay agent information.

Examples

The following example configures the device to keep the relay agent information contained in a DHCP message.

```
device(config)# ip dhcp relay information policy keep
```

The following example configures the device to drop the relay agent information contained in a DHCP message.

```
device(config)# ip dhcp relay information policy drop
```

ip directed-broadcast

Enables directed broadcast forwarding.

Syntax

ip directed-broadcast

no ip directed-broadcast

Command Default

Directed broadcast forwarding is disabled by default.

Modes

Global configuration mode

Usage Guidelines

A Smurf attack relies on the intermediary to broadcast ICMP echo request packets to hosts on a target subnet. When the ICMP echo request packet arrives at the target subnet, it is converted to a Layer 2 broadcast and sent to the connected hosts. This conversion takes place only when directed broadcast forwarding is enabled on the device. To avoid being an intermediary in a Smurf attack, make sure forwarding of directed broadcasts is disabled on the device.

The **no** form of the command disables directed broadcast forwarding.

Examples

The following example enables directed broadcast forwarding.

```
device(config)# ip directed-broadcast
```

ip dns

Configures the IPv4 Domain Name System (DNS).

Syntax

ip dns { **domain-list** *domain-name* | **server-address** *ip-address* [*ip-address*...] }

no ip dns { **domain-list** *domain-name* | **server-address** *ip-address* [*ip-address*...] }

Command Default

IP DNS is not configured.

Parameters

domain-list
Configures a list of DNS domains.

domain-name
The domain name.

server-address
Configures the DNS server IPv4 address.

ip-address
The IPv4 address of the DNS server. You can configure up to a maximum of four IP addresses separated by a space.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the DNS configurations.

Examples

The following example shows how to configure an IPv4 address for a DNS server.

```
device(config)# ip dns server-address 192.168.10.1 192.168.100.1
```

The following example shows how to configure the DNS domain-list.

```
device(config)# ip dns domain-list company.com
```

ip dscp-remark

Enables remarking of the differentiated services code point (DSCP) field for all IPv4 packets.

Syntax

ip dscp-remark *dscp-value*

no ip dscp-remark *dscp-value*

Command Default

DSCP remarking is disabled.

Parameters

dscp-value

Specifies the DSCP value ranges you are remarking.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of this command disables DSCP remarking.

In interface configuration mode, the command enables DSCP remarking for the given port. The configuration can be done on a physical port, LAG, and VE port.

If DHCP snooping is enabled, you cannot globally enable DSCP remarking. When you enter the global configuration **ip dscp-remark** command, the following error message is displayed.

```
Error: DHCP Snooping is configured on the system. Cannot enable DSCP remarking
```

Examples

The following example globally enables DSCP remarking on all IPv4 packets when the DSCP bit value is 40:

```
Device(config)# ip dscp-remark 40
```

The following example enables DSCP remarking on all IPv4 packets received on a specific port when the DSCP bit value is 50:

```
Device(config)# interface ethernet1/1/1
Device(config-if-e1000-1/1/1)# ip dscp-remark 50
```

ip follow-ingress-vrf

Configures the SNMP reply to be sent either through default-VRF using management port or management-VRF based on the SNMP-request's ingress.

Syntax

ip follow-ingress-vrf

no ip follow-ingress-vrf

Command Default

By default, when there is a conflict in route, SNMP-reply is sent through management-VRF irrespective of the VRF in which SNMP-Request is received.

Modes

Global configuration mode

Usage Guidelines

When management-vrf is configured and if there is a conflict in route between default-VRF using management port and management-VRF, UDP based module like SNMP, TFTP will always send packet through management-VRF based route. That is, by default, when there is a conflict in route, SNMP-reply is sent through management-VRF irrespective of the VRF in which SNMP-Request is received. Use this command if SNMP-Reply is to be sent on the VRF in which SNMP-Request is received.

The **no** form of the command configures the SNMP-Reply to be sent through management-VRF even when there is a conflicting route between default-VRF using management port and management-VRF .

Examples

The following example configures the SNMP-Reply to be sent based on SNMP-Request's VRF.

```
device(config)# ip follow-ingress-vrf
```

History

Release version	Command history
08.0.30e	This command was introduced.

ipg

Configures Interpacket Gap (IPG) on an Ethernet interface. An IPG is a configurable time delay between successive data packets.

Syntax

ipg *bit-time*

no ipg *bit-time*

Command Default

The default is 96 bit time.

Parameters

bit-time

Specifies the IPG bit time. The bit time ranges from 48 to 120 bit times in multiples of 8. The default value is 96.

Modes

Interface configuration mode

Usage Guidelines

An IPG is a configurable time delay between successive data packets. When an IPG is applied to a LAG, it applies to all ports in the LAG. When you are creating a new LAG, the IPG setting on the primary port is automatically applied to the secondary ports.

This feature is supported on 10/100/1000M ports.

The **no** form of the command removes the configured Interpacket Gap (IPG) bit time.

You can set IPG for a list of range of ports as well.

Examples

The following example shows how to configure an IPG of 112 on Ethernet interface 1/1/21.

```
device(config)# interface ethernet 1/1/21
device(config-if-e1000-1/1/21)# ipg 112
```

ipg-gmii

Configures IPG on a Gbps Ethernet port for 1-Gbps Ethernet mode.

Syntax

ipg-gmii *bit-time*

no ipg-gmii *bit-time*

Command Default

The default is 96 bits time (96 nanoseconds).

Parameters

bit-time

Specifies Inter-Packet-Gap in bits-time. The value can range from 48 to 112. The default value is 96.

Modes

Interface configuration mode

Usage Guidelines

This command is supported only on FSX devices.

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

Examples

The following example shows how to configure the IPG.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipg-gmii 100
IPG 120(112) has been successfully configured for ports 1/1 to 1/12
```

ipg-mii

Configures IPG on a Gbps Ethernet port for 10/100M mode.

Syntax

ipg-mii *bit-time*

no ipg-mii *bit-time*

Command Default

The default is 96 bit time.

Parameters

bit-time

Specifies the Inter-Packet-Gap in bits time. The value can range from 12 to 124. The default is 96 bit time.

Modes

Interface configuration mode

Usage Guidelines

This command is supported only on FSX devices.

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

Examples

The following example shows how to set the IPG configuration.

```
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipg-mii 120
IPG 120(120) has been successfully configured for ports 1/1 to 1/12
```

ipg-xgmii

Configures Interpacket Gap (IPG) on a 10 Gbps Ethernet interface.

Syntax

ipg-xgmii *bit-time*

no ipg-xgmii *bit-time*

Command Default

The default is 96 bit time (9.6 nanoseconds).

Parameters

bit-time

Specifies Inter-Packet-Gap in bits-time. The value can range from 96 to 192. The default is 96 bit time.

Modes

Interface configuration mode

Usage Guidelines

This command is supported only on FSX devices.

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

Examples

The following example shows hot to set the IPG configuration.

```
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ipg-xgmii 120
IPG 120(128) has been successfully configured for port 1/1
```

ip helper-use-responder-ip

Configures the Brocade device so that a BOOTP or DHCP reply to a client contains the server IP address as the source address instead of the router IP address.

Syntax

ip helper-use-responder-ip

no ip helper-use-responder-ip

Modes

Global configuration mode

Examples

The following example retains the responder source IP in the reply.

```
device(config)# ip helper-use-responder-ip
```

ip hitless-route-purge-timer

Configures the timer to set the duration for which the routes should be preserved after switchover.

Syntax

ip hitless-route-purge-timer *seconds*

no ip hitless-route-purge-timer *seconds*

Command Default

The default timer setting is 45 seconds.

Parameters

seconds

Specifies the time after switchover to start IPv4 route purge. The value can range from 2 to 600 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the configured value and sets the timer to the default 45 seconds.

This command is supported only on the FastIron X Series devices (FSX 800 and FSX 1600).

Examples

The following example shows how to set the IPv4 hitless purge timer to 60 seconds.

```
device(config)# ip hitless-route-purge-timer 60
```

ip icmp burst-normal

Configures the device to drop ICMP packets when excessive number of packets are encountered.

Syntax

ip icmp burst-normal *num-packets* **burst-max** *num-packets* **lockup** *time*

no ip icmp burst-normal *num-packets* **burst-max** *num-packets* **lockup** *time*

ip icmp attack-rate burst-normal *num-packets* **burst-max** *num-packets* **lockup** *time*

no ip icmp attack-rate burst-normal *num-packets* **burst-max** *num-packets* **lockup** *time*

Command Default

Threshold values for ICMP packets are configured.

Parameters

num-packets

Configures the number of packets per second in normal burst mode. Valid values are from 1 through 100,000 packets per second.

NOTE
For the Brocade ICX 7750, the value is in Kbps.

burst-max *num-packets*

Specifies the number of packets per second in maximum burst mode. Valid values are 1 through 100,000 packets per second.

NOTE
For the Brocade ICX 7750, the value is in Kbps.

lockup *time*

Configures the lockup period in seconds. Valid values are from 1 through 10,000 seconds.

attack-rate

Configures the attack rate. This is specific to the Brocade ICX 7750.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

You can configure the Brocade device to drop ICMP packets when excessive number of packets are encountered, as is the case when the device is the victim of a Smurf attack. You can set threshold values for ICMP packets that are targeted at the router itself or passing through an interface, and drop them when the thresholds are exceeded.

For Layer 3 router code, if the interface is part of a VLAN that has a router VE, you must configure ICMP attack protection at the VE level. When ICMP attack protection is configured at the VE level, it will apply to routed traffic only. It will not affect switched traffic.

> **NOTE**
> You must configure VLAN information for the port before configuring ICMP attack protection. You cannot change the VLAN configuration for a port on which ICMP attack protection is enabled.

The **no** form of the command removes the configured threshold value.

Examples

The following example sets threshold values for ICMP packets targeted at the router.

```
device(config)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

The following example sets threshold values for ICMP packets received on interface 3/1/1.

```
device(config)# interface ethernet 3/1/1
device(config-if-e1000-3/1/1)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

The following example sets the threshold value for ICMP packets received on VE 31.

```
device(config)# interface ve 31
device(config-vif-31)# ip icmp burst-normal 5000 burst-max 10000 lockup 300
```

ip icmp echo broadcast-request

Enables an ICMP echo response caused by a broadcast echo request.

Syntax

ip icmp echo broadcast-request

no ip icmp echo broadcast-request

Command Default

By default, Brocade devices are enabled to respond to broadcast ICMP echo packets, which are ping requests.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the response to broadcast ICMP echo packets (ping requests).

Examples

The following example enables an ICMP echo response caused by a broadcast echo request.

```
device(config)# ip icmp echo broadcast-request
```

ip icmp redirects

Enables IPv4 ICMP redirect messages.

Syntax

ip icmp redirects

no ip icmp redirects

Command Default

By default, IP ICMP redirect at the global level is disabled and a Brocade Layer 3 switch does not send an ICMP redirect message to the source of a misdirected packet in addition to forwarding the packet to the appropriate router.

Modes

Global configuration mode

VE interface configuration mode

Usage Guidelines

You can enable and disable IPv4 ICMP redirect messages globally or on individual Virtual Ethernet (VE) interfaces, but not on individual physical interfaces.

NOTE
Some FSX devices do not generate ICMP redirect and network unreachable messages.

NOTE
The device forwards misdirected traffic to the appropriate router, even if you disable the redirect messages.

The **no** form of the command removes the ICMP redirect control.

Examples

The following example configures the IP redirect messages at the global level.

```
device(config)# ip icmp redirects
```

The following example configures the IP redirect messages on a VE interface.

```
device(config)# interface ve 10
device(config-vif-10)# ip icmp redirects
```

ip icmp unreachable

Enables sending ICMP unreachable messages.

Syntax

ip icmp unreachable { **administration** | **fragmentation-needed** | **host** | **network** | **port** | **protocol** | **source-route-fail**}

no ip icmp unreachable { **administration** | **fragmentation-needed** | **host** | **network** | **port** | **protocol** | **source-route-fail**}

Command Default

By default, when a Brocade device receives an IP packet that the device cannot deliver, the device sends an ICMP unreachable message back to the host that sent the packet.

Parameters

administration
Sends the ICMP unreachable message when the packet is dropped by the device due to a filter or ACL configured on the device.

fragmentation-needed
Sends the ICMP unreachable message when the packet has the Do not Fragment bit set in the IP Flag field, but the device cannot forward the packet without fragmenting it.

host
Sends the ICMP unreachable message when the destination network or subnet of the packet is directly connected to the device, but the host specified in the destination IP address of the packet is not on the network.

network
Sends the ICMP unreachable message when the destination network is

port
Sends the ICMP unreachable message when the destination host does not have the destination TCP or UDP port specified in the packet. In this case, the host sends the ICMP port unreachable message to the device, which in turn sends the message to the host that sent the packet.

protocol
Sends the ICMP unreachable message when TCP or UDP on the destination host is not running. This message is different from the port unreachable message, which indicates that the protocol is running on the host but the requested protocol port is unavailable.

source-route-fail
Sends the ICMP unreachable message when the device received a source-routed packet but cannot locate the next hop IP address indicated in the packet Source-Route option.

Modes

Global configuration mode

Usage Guidelines

You can disable the Brocade device from sending these types of ICMP messages on an individual basis.

> **NOTE**
> Disabling an ICMP unreachable message type does not change the Brocade device ability to forward packets. Disabling ICMP unreachable messages prevents the device from generating or forwarding the unreachable messages.

The **no** form of the command disables the ICMP unreachable messages.

Examples

The following example enables the ICMP unreachable message when the destination network or subnet of the packet is directly connected to the device, but the host specified in the destination IP address of the packet is not on the network.

```
device(config)# ip icmp unreachable host
```

ip igmp group-membership-time

Specifies how long an IGMP group remains active on an interface in the absence of a group report.

Syntax

ip igmp group-membership-time *num*

no ip igmp group-membership-time *num*

Command Default

By default, a group will remain active on an interface for 260 seconds in the absence of a group report.

Parameters

num

Number in seconds, from 5 through 26000.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of this command resets the group membership time interval to the default of 260 seconds.

Group membership time defines how long a group will remain active on an interface in the absence of a group report.

Examples

This example specifies an IGMP (V1 and V2) membership time of 240 seconds.

```
Device(config)# ip igmp group-membership-time 240
```

ip igmp max-response-time

Defines how long a device waits for an IGMP response from an interface before determining that the group member on that interface is down and removing the interface from the group.

Syntax

ip igmp max-response-time *num*

no ip igmp max-response-time *num*

Command Default

The device waits 10 seconds.

Parameters

num

Number, in seconds, from 1 through 25. The default is 10.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of this command resets the maximum response time interval to the default of 10 seconds.

Examples

To define

This example changes the IGMP (V1 and V2) maximum response time to 8 seconds.

```
Device(config)# ip igmp max-response-time 8
```

ip igmp port-version

Configures an IGMP version recognized by a physical port that is a member of a virtual routing interface.

Syntax

ip igmp port-version *version-number* **ethernet** *port-number* [**to ethernet** *port-number*[**ethernet** *port-number...*]]

no ip igmp port-version *version-number* **ethernet** *port-number* [**to ethernet** *port-number*[**ethernet** *port-number...*]]

Command Default

IGMP Version 2 is enabled.

Parameters

version-number

Specifies the version number: 1, 2, or 3. Version 2 is the default.

ethernet *port-number*

Specifies the physical port within a virtual routing interface.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the default; IGMP Version 2 is enabled.

Examples

This example enables IGMP Version 3 on a physical port that is a member of a virtual routing interface. It first enables IGMP Version 2 globally, then enables Version 3 on ports 1/3 through 1/7 and port e2/9. All other ports in this virtual routing interface are configured with IGMP Version 2.

```
device(config)#interface ve 3
device(config-vif-3)# ip igmp version 2
device(config-vif-3)# ip igmp port-version 3 e1/3 to e1/7 e2/9
```

ip igmp proxy

Configures IGMP proxy on an interface

Syntax

ip igmp proxy [**group-filter***access-list*]

no ip igmp proxy [**group-filter***access-list*]

Command Default

IGMP proxy is not enabled.

Parameters

group-filter

Specifies filtering out groups in proxy report messages.

access-list

Specifies the access list name or number you want filtered out.

Modes

Interface configuration mode.

Usage Guidelines

The **no** form of this command disables IGMP proxy on an interface.

IGMP proxy is supported only in PIM dense environments where there are IGMP clients connected to the Brocade device. PIM DM must be enabled in passive mode.

IGMP proxy is not supported on interfaces on which PIM sparse mode (SM) or Source Specific Multicast (SSM) is enabled.

Enter the **ip igmp proxy** command without the **group-filter** keyword to remove the group-filter association without disabling the proxy.

Examples

This example enables IGMP proxy on an interface. It first shows how to configure PIM globally, configure an IP address that will serve as the IGMP proxy for an upstream device on interface 1/3, enable PIM passive on the interface, and then enable IGMP proxy.

```
device(config)#router pim
device(config)#interface ethernet 1/3/3
device(config-if-e1000-1/3)#ip address 10.95.5.1/24
device(config-if-e1000-1/3)#ip pim passive
device(config-if-e1000-1/3)#ip igmp proxy
```

The following example filters out the ACL1 group in proxy report messages.

```
device(config)#router pim
device(config)#interface ethernet 1/3/3
device(config-if-e1000-1/3)#ip address 10.95.5.1/24
device(config-if-e1000-1/3)#ip pim passive
device(config-if-e1000-1/3)#ip igmp proxy group-filter ACL1
```

ip igmp query-interval

Defines how often a device queries an interface for IGMP group membership.

Syntax

ip igmp query-interval *num*

no ip igmp query-interval *num*

Command Default

The query interval is 125 seconds

Parameters

num

Number in seconds, from 2 through 3600. The default is 125.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of this command resets the query interval to the default of 125 seconds.

You must specify a query-interval value that is a little more than twice the group membership time. You can configure the `ip igmp group-membership-time` command to specify the IGMP group membership time.

Examples

This example sets the IGMP query interval to 120 seconds.

```
Device(config)# ip igmp query-interval 120
```

ip igmp tracking

Enables tracking and fast leave on an interface.

Syntax

ip igmp tracking

no ip igmp tracking

Command Default

Tracking and fast leave are disabled.

Modes

Interface configuration mode.

Usage Guidelines

The **no** form of this command restores the default; tracking and fast leave are disabled.

The IGMP Version 3 fast leave feature is supported in include mode but does not work in exclude mode.

Examples

This example enables tracking and fast leave on a virtual routing interface.

```
Device(config)# interface ve 13
Device(config-vif-13)# ip igmp tracking
```

This example enables tracking and fast leave on a physical interface.

```
Device(config)# i(config)#interface ethernet 1/2/2
Device(config-if-e10000-1/2/2)# ip igmp tracking
```

ip igmp version

Specifies the IGMP version on a device.

Syntax

ip igmp version *version-number*

no ip igmp version *version-number*

Command Default

IGMP Version 2 is enabled.

Parameters

version-number

Specifies the version number: 1, 2, or 3. Version 2 is the default.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of this command restores the default; IGMP Version 2 is enabled.

Configure the **ip igmp port-version** command to configure an IGMP version recognized by a physical port that is a member of a virtual routing interface.

Examples

The following example enables IGMP Version 3 globally.

```
device# configure terminal
device(config)# ip igmp version 3
```

The following example, in interface configuration mode, enables IGMP Version 3 for a physical port.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(config-if-1/5)# ip igmp version 3
```

The following example, in interface configuration mode, enables IGMP Version 3 for a virtual routing interface on a physical port.

```
device# configure terminal
device(config)# interface ve 3
device(config-vif-1)# ip igmp version 3
```

ip max-mroute

Configures the maximum number of IPv4 multicast routes that are supported.

Syntax

ip max-mroute *num*

no ip max-mroute *num*

Command Default

No maximum number of supported routes is configured.

Parameters

num

Configures the maximum number of multicast routes supported.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command restores the default (no maximum number of supported routes is configured).

Examples

The following example configures the maximum number of 20 supported IPv4 multicast routes on the VRF named my_vrf.

```
Device(config)# vrf my_vrf
Device(config)# address-family ipv4
Device(config-vrf)# ip max-mroute 20
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute

Configures a directly connected static IPv4 multicast route.

Syntax

ip mroute [**vrf** *vrf-name*] *ip-address ip-address mask* { **ethernet** *stackid* / *slot* / *portnum* | **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

no ip mroute [**vrf** *vrf-name*] *ip-address ip-address mask* { **ethernet** *stackid* / *slot* / *portnum*| **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default

No static IPv4 multicast route is configured.

Parameters

vrf *vrf-name*
Configures a static mroute for this virtual routing and forwarding (VRF) route.

ip-address ip-address mask
Configures the destination IPv4 address and prefix for which the route should be added.

ethernet *stackid* / *slot* /*portnum*
Configures an Ethernet interface as the route path.

ve *num*
Configures a virtual interface as the route path.

tunnel *num*
Configures a tunnel interface as the route path.

cost
Configures a metric for comparing the route to other static routes in the static route table that have the same destination. The range is 1-16; the default is 1.

distance *distance-value*
Configures the route's administrative distance. The range is 1-255; the default is 1.

name *name*
Name for this static route.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command deletes a previously configured directly connected static multicast route.

Connected routes on PIM enabled interfaces are automatically added to the mRTM table.

Examples

The following example configures a directly connected mroute to network 10.1.1.0/24 on interface ve 10.

```
Device(config-vrf)# ip mroute 10.1.1.0 255.255.255.0 ve 10
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute (next hop)

Configures a static IPv4 multicast route (mroute) with a next hop..

Syntax

ip mroute [**vrf** *vrf-name*] *ip-address ip-address mask next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

no ip mroute [**vrf** *vrf-name*] *ip-address ip-address mask next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default

No next-hop static IPv4 multicast route is configured.

Parameters

vrf *vrf-name*
: Configures a static mroute for this virtual routing and forwarding (VRF) route.

ip-address ip-address mask
: Configures the destination IPv4 address and prefix for which the route should be added.

next-hop address
: Configures a next-hop address as the route path.

cost
: Configures a metric for comparing the route to other static routes in the static route table that have the same destination. The range is 1-16; the default is 1.

distance *distance-value*
: Configures the route's administrative distance. The range is 1 through 255; the default is 1.

name *name*
: Name for this static route.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command deletes a previously configured next-hop static IPv4 multicast route.

Examples

The following example configures a next-hop static multicast IPv4 route to network 10.1.1.0/24 with next hop 10.2.1.1.

```
Device(config-vrf)# ip mroute 10.1.1.0 255.255.255.0 10.2.1.1
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute next-hop-enable-default

Enables the option to use the default multicast route (mroute) to resolve a static IPv4 mroute next hop.

Syntax

ip mroute [**vrf** *vrf-name*] **next-hop-enable-default**

no ip mroute [**vrf** *vrf-name*] **next-hop-enable-default**

Command Default

Static mroutes are not resolved using the default mroute.

Parameters

vrf *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command disables the default IPv4 mroute option for next hops.

Examples

The following example enables the use of the default mroute to resolve a static IPv4 mroute next hop:

```
Device(config-vrf)# ip mroute next-hop-enable-default
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip mroute next-hop-recursion

Configures the recursion level when using static mroutes to resolve a static mroute next hop.

Syntax

ip mroute [**vrf** *vrf-name*] **next-hop-recursion** *num*

no ip mroute [**vrf** *vrf-name*] **next-hop-recursion**

Command Default

The recursion level for resolving a static mroute next hop is 3.

Parameters

vrf *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

num

Specifies the recursion level used to resolve a static mroute next hop. The range of possible values is from 1 to 10. This is not used in the **no** form.

Modes

VRF configuration mode

Usage Guidelines

The **no** form restores the default recursion level for resolving a static mroute next hop, which is 3. You do not specify a value for the recursion level.

Examples

The following example configures the recursion level for resolving a static mroute next hop to 7:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ip mroute next-hop-recursion 7
```

The following example configures the recursion level for resolving a static mroute next hop to 2:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ip mroute next-hop-recursion 2
```

The following example restores the default recursion level of 3 for resolving a static mroute next hop:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# no ip mroute next-hop-recursion
```

History

Release version	Command history
8.0.10a	This command was introduced.

ip multicast

Configures the IGMP mode on a specific VLAN or on all VLANs on a device as active or passive.

Syntax

ip multicast [**vlan** | *vlan-id*] [**active** | **passive**]

no ip multicast

Command Default

IGMP mode is passive.

Parameters

vlan *vlan-id*

Specifies a VLAN.

active

Configures IGMP active mode, that is, the device actively sends out IGMP queries to identify multicast groups on the network and makes entries in the IGMP table based on the group membership reports it receives.

passive

Configures IGMP passive mode, that is, the device does not send queries but forwards reports to the router ports that receive queries. When passive mode is configured on a VLAN, queries are forwarded to the entire VLAN.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

The **no** form of this command returns the device to the previous IGMP mode.

When entered without the **vlan** keyword, this command configures active or passive IGMP mode on all VLANs.

Routers in the network generally handle mode. Configure active IGMP mode only on a device is in a standalone Layer 2 Switched network with no external IP multicast router attachments. If you want to configure active IGMP mode on a device in such a network, you should do so on only one device and leave the others configured as passive.

The IGMP mode configured on a VLAN overrides the mode configured globally.

Examples

The following example globally configures IGMP mode as active.

```
device#configure terminal
device(config)#ip multicast active
```

This example configures IGMP mode as active on VLAN 20.

```
device#configure terminal
device(config)#config vlan 20
device(config-vlan-20)#ip multicast active
```

ip multicast age-interval

Configures the time that group entries can remain in an IGMP group table on a specific VLAN or on all VLANs.

Syntax

ip multicast age-interval [**vlan** *vlan-id*] *interval*

no ip multicast age-interval [**vlan** *vlan-id*] *interval*

Command Default

Group entries can remain in the IGMP group table for up to 260 seconds.

Parameters

vlan *vlan-id*

Specifies a VLAN.

interval

Specifies time, in seconds, that group entries can remain in the IGMP group table. The range is 20 through 26000 seconds. The default is 260 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default age interval to 260 seconds.

When entered without the **vlan** keyword, this command configures the time that group entries can remain in an IGMP group table on all VLANs.

When a device receives a group membership report it makes an entry for that group in the IGMP group table. You can configure the **ip multicast age-interval** to specify how long the entry can remain in the table before the device receives another group membership report. When multiple devices are connected, they must all be configured for the same age interval, which must be at least twice the length of the query interval, so that missing one report does not stop traffic.

Non-querier age intervals must be the same as the age interval of the querier.

Examples

This example configures the IGMP group-table age interval to 280 seconds.

```
device#configure terminal
device(config)#ip multicast age-interval 280
```

ip multicast disable-flooding

Disables the flooding of unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN.

Syntax

ip multicast disable-flooding

no ip multicast disable-flooding

Command Default

The device floods unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN.

Modes

Global configuration mode

Usage Guidelines

NOTE
Disabling the flooding of unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN is supported only on the following platforms:

- The Brocade ICX 6650
- The Brocade ICX 7750 (standalone and stacking)
- The Brocade ICX 7450 (standalone and stacking)
- The Brocade ICX 7250 (standalone and stacking)

The **no** form of this command enables the flooding of unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN.

Support for this command on the Brocade ICX 7750 was introduced in FastIron 8.0.10d. In releases prior to FastIron 8.0.30, support for this command on the Brocade ICX 7750 was for devices in standalone mode only.

Support for this command on the Brocade ICX 7450 and Brocade ICX 7250 was introduced in FastIron 8.0.30.

After the hardware forwarding database (FDB) entry is made, the multicast traffic is switched only to the VLAN hosts that are members of the multicast group. This can avoid congestion and loss of traffic on the ports that have not subscribed to this IPv4 multicast traffic.

Examples

The following example disables flooding of unregistered IPv4 multicast frames.

```
Device(config)# ip multicast disable-flooding
```

History

Release version	Command history
08.0.01	This command was introduced.

ip multicast leave-wait-time

Configures the wait time before stopping traffic to a port when a leave message is received.

Syntax

ip multicast leave-wait-time *num*

no ip multicast leave-wait-time *num*

Command Default

The wait time is 2 seconds.

Parameters

num

Specifies the time, in seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 1 through 5 seconds. The default is 2 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default wait time.

The device sends group-specific queries once per second to ask if any client in the same port still needs this group. Because of internal timer granularity, the actual wait time is between n and (n+1) seconds (n is the configured value).

Examples

This example configures the maximum time a client can wait before responding to a query to 1 second.

```
Device(config)#ip multicast leave-wait-time 1
```

ip multicast max-response-time

Sets the maximum number of seconds a client can wait before responding to a query sent by the device.

Syntax

ip multicast max-response-time *interval*

no ip multicast max-response-time *interval*

Command Default

The wait time is 10 seconds.

Parameters

interval

Specifies the maximum time, in seconds, a client can wait before responding to a query sent by the switch. The range is 1 through 10 seconds. The default is 10 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default maximum interval.

Examples

This example configures the maximum time a client can wait before responding to a query to 5 seconds.

```
Device(config)#ip multicast max-response-time 5
```

ip multicast mcache-age

Configures the time for an mcache to age out when it does not receive traffic.

Syntax

ip multicast mcache-age *num*

no ip multicast mcache-age

Command Default

The mcache ages out after the default age-out interval, which is 180 seconds for FSX 800/1600, ICX 7750, ICX 7450, and ICX 7250 devices, and 60 seconds for all other devices.

Parameters

num

Specifies the time, in multiples of 60 seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 60 through 3600 seconds, in multiples of 60.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default mcache age-out time.

Multicast traffic is hardware switched. One minute before aging out an mcache, the device mirrors a packet of this mcache to CPU to reset the age. If no data traffic arrives within 60 seconds, this mcache is deleted. Configuring a lower age-out time removes resources consumed by idle streams quickly, but it mirrors packets to CPU often. Configure a higher value only when data streams are arriving consistently.

Examples

This example configures the time for an mcache to age out to 180 seconds.

```
Device(config)#ip multicast mcache-age 180
```

ip multicast query-interval

Configures how often the device sends general queries when IP multicast traffic reduction is set to active mode.

Syntax

ip multicast query-interval *interval*

no ip multicast query-interval *interval*

Command Default

The query interval is 125 seconds.

Parameters

interval

Specifies the time, in seconds, between queries. The range is 10 through 3600 seconds. The default is 125 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the query interval to 125 seconds.

You can configure this command only when IP multicast traffic reduction is set to active IGMP snooping mode.

When multiple queries are connected, they must all be configured for the same interval.

Examples

This example configures the time between queries to 120 seconds.

```
Device(config)#ip multicast query-interval 120
```

ip multicast report-control

Limits report forwarding within the same multicast group to no more than once every 10 seconds.

Syntax

ip multicast report-control

no ip multicast report-control

Command Default

A device in passive mode forwards reports and leave messages from clients to the upstream router ports that are receiving queries.

Modes

Global configuration mode

Usage Guidelines

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

> **NOTE**
> This feature applies to IGMP V2 only. The leave messages are not rate limited.

This rate-limiting does not apply to the first report answering a group-specific query.

Configure this command to alleviate report storms from many clients answering the upstream router query.

The **ip multicast report-control** command was formerly named **ip igmp-report-control** . You can still configure the command as **ip igmp-report-control** ; however, it is renamed when you configure the **show configuration** command.

Examples

This example limits the rate of report forwarding within the same multicast group.

```
Device(config)#ip multicast report-control
```

ip multicast verbose-off

Turns off the error or warning messages displayed by the device when it runs out of software resources or when it receives packets with the wrong checksum or groups.

Syntax

ip multicast verbose-off

no ip multicast verbose-off

Command Default

Error and warning messages are displayed.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores display of error and warning messages .

Error and warning messages are rate-limited.

Examples

This example turns off error or warning messages .

```
Device(config)#ip multicast verbose-off
```

ip multicast version

Configures the IGMP version for snooping globally.

Syntax

ip multicast version [**2** | **3**]

no ip multicast version

Command Default

IGMP version 2 is configured.

Parameters

2

Configures IGMP version 2.

3

Configures IGMP version 3.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the version to IGMP version 2.

If Layer 3 multicast routing is enabled on the device, Layer 2 IGMP snooping is automatically enabled.

See the description of the **multicast version** command for information on how to configure the IGMP version on a VLAN.

See the description of the **multicast port-version** command for information on how to configure the IGMP version on an individual port

Examples

This example specifies IGMP version 3 on a device.

```
Device(config)#ip multicast version 3
```

ip multicast-routing rpf-check mac-movement

Triggers Reverse Path Forwarding (RPF) check on MAC movement for directly connected sources and sends a MAC address movement notification to the Protocol Independent Multicast (PIM) module which results in PIM convergence.

Syntax

ip multicast-routing rpf-check mac-movement

no ip multicast-routing rpf-check mac-movement

Command Default

RPF check on MAC movement for directly connected sources is not enabled.

Modes

Global configuration mode

Usage Guidelines

PIM convergence on MAC movement is applicable only in a topology where the multicast source port and PIM routers are in the same Layer 2 domain.

The **ip multicast-routing rpf-check mac-movement** command is not supported on the Brocade ICX 6650, Brocade ICX 7250, and FSX 800/FSX 1600 devices.

The **no** form of the command disables RPF check on MAC movement for directly connected sources.

Examples

The following example configures RPF check on MAC movement for directly connected sources.

```
device(config)# ip multicast-routing rpf-check mac-movement
```

History

Release version	Command history
08.0.10h	This command was introduced.
08.0.30	Support for the **ip multicast-routing rpf-check mac-movement** command was added in 08.0.30 and later releases.

ip multicast-nonstop-routing

Globally enables multicast non-stop routing for all virtual routing and forwarding (VRF) instances.

Syntax

ip multicast-nonstop-routing

no ip multicast-nonstop-routing

Command Default

Multicast non-stop routing is not enabled on VRFs.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default non-stop routing.

Examples

The following example globally enables multicast non-stop routing for all VRFs.

```
device#configure terminal
device(config)#ip multicast-nonstop-routing
```

ip pcp-remark

Enables remarking of the priority code point (PCP) field in the VLAN header for all received tagged packets.

Syntax

ip pcp-remark *pcp-value*

no ip pcp-remark *pcp-value*

Command Default

PCP remarking is disabled.

Parameters

pcp-value

Specifies the PCP value ranges you are remarking.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of this command disables PCP remarking.

In Interface configuration mode, the command enables PCP remarking for each port. The command can be configured only on Layer 2 ports. The configuration can be done on a physical port, LAG, and VE port.

Examples

The following example globally enables remarking of received tagged packets when the PCP bit value is 4.

```
Device(config)# ip pcp-remark 4
```

The following example enables remarking of received tagged packets on a specific port when the PCP bit value is 5.

```
Device(config)# interface ethernet1/1/1
Device(config-if-e1000-1/1/1)# ip pcp-remark 5
```

ip pim

Configures PIM in Dense mode on an interface.

Syntax

ip pim [**passive**]

no ip pim [**passive**]

Command Default

PIM is not enabled.

Parameters

passive

Specifies PIM passive mode on the interface.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command disables PIM.

You must enable PIM globally before you enable it on an interface.

You must enable PIM on an interface before you can configure PIM passive on it.

Support for the **ip pim passive** command is implemented at Layer 3 interface (Ethernet or virtual Ethernet) level.

Because the loopback interfaces are never used to form PIM neighbors, the **ip pim passive** command is not supported on loopback interfaces.

The sent and received statistics of a PIM Hello message are not changed for an interface while it is configured as PIM passive.

Examples

This example enables PIM globally, then enables it on interface 3.

```
Device(config)# router pim
Device(config-pim-router)# interface ethernet 1/1/3
Device(config-if-e10000-1/1/3)# ip address 207.95.5.1/24
Device(config-if-e10000-1/1/3)# ip pim
```

This example enables PIM passive on an interface.

```
Device(config)# router pim
device(config-pim-router)#exit
Device(config)#interface ethernet 2
Device(config-if-e1000-2)#ip pim
Device(config-if-e1000-2)#ip pim passive
Device(config-if-e1000-2)#exit
Device(config)#interface ve 2
Device(config-vif-2)#ip pim-sparse
Device(config-vif-2)#ip pim passive
Device(config-vif-2)#exit
```

ip pim border

Configures PIM parameters on an interface on a PIM Sparse border.

Syntax

ip pim border

no ip pim border

Command Default

The interface is not configured as a border device.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command removes the boundary on a PIM-enabled interface.

You can configure this command only in a PIM Sparse domain, that is, you must configure the **ip pim-sparse** command before you configure the **ip pim border** command.

Examples

This example adds an IPv4 interface to port 1/2/2, enables PIM Sparse on the interface and configures it as a border device.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e10000-1/2/2)# ip address 207.95.7.1 255.255.255.0
Device(config-if-e10000-1/2/2)# ip pim-sparse
Device(config-if-e10000-1/2/2)# ip pim border
```

ip pim dr-priority

Configures the designated router (DR) priority on IPv4 interfaces.

Syntax

ip pim dr-priority *priority-value*

no ip pim dr-priority *priority-value*

Command Default

The default DR priority value is 1.

Parameters

priority-value

Specifies the DR priority value as an integer. The range is 0 through 65535.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the default DR priority value, 1.

You must enable PIM globally before you enable it on an interface.

You can configure the **ip pim dr-priority** command in either Dense mode (DM) or Sparse mode (SM).

If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IP address on that subnet is elected as the DR.

The DR priority information is used in the DR election only if all the PIM devices connected to the subnet support the DR priority option. If at least one PIM device on the subnet does not support this option, the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IP address on the subnet is declared the DR regardless of the DR priority values.

Examples

This example configures a DR priority value of 50.

```
device(config)# interface ethernet 1/3/24
device(config-if-e10000-1/3/24)# ip pim dr-priority 50
```

This example configures a DR priority value of 50.

```
device(config)# interface ethernet 1/3/24
device(config-if-e10000-1/3/24)# ip pim dr-priority 50
```

ip pim neighbor-filter

Determines which devices can become PIM neighbors.

Syntax

ip pim neighbor-filter { *acl-name* | *acl-id* }

no ip pim neighbor-filter { *acl-name* | *acl-id* }

Command Default

Neighbor filtering is not applied on the interface.

Parameters

acl-name

Specifies an ACL as an ASCII string.

acl-id

Specifies either a standard ACL as a number in the range 1 to 99 or an extended ACL as a number in the range 100 to 199.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command removes any neighbor filtering applied on the interface.

You must enable PIM globally before you enable it on an interface.

You can configure the **ip pim neighbor-filter** command in either Dense mode (DM) or Sparse mode (SM).

Configure the **access-list** command to create an access-control list (ACL)that specifies the devices you want to permit and deny participation in PIM

Examples

This example prevents the host from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ip pim neighbor-filter
```

This example configures an ACL named 10 to deny a host and then prevents that host, 10.10.10.2, identified in that ACL from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# access-list  10  deny  host 10.10.10.2
Device(config)# access-list  10  permit any
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ip pim neighbor-filter 10
```

History

Release version	Command history
8.0.20a	This command was introduced.

ip pimsm-snooping

Enables PIM Sparse mode (SM) traffic snooping globally.

Syntax

ip pimsm-snooping

no ip pimsm-snooping

Command Default

PIM SM traffic snooping is disabled.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

The **no** form of this command disables PIM SM traffic snooping.

The device must be in passive mode before it can be configured for PIM SM snooping.

Use PIM SM snooping only in topologies where multiple PIM sparse routers connect through a device. PIM SM snooping does not work on a PIM dense mode router that does not send join messages and on which traffic to PIM dense ports is stopped. A PIM SM snooping-enabled device displays a warning if it receives PIM dense join or prune messages.

When PIM SM snooping is enabled globally, you can override the global setting and disable it for a specific VLAN.

Examples

This example shows how to enable PIM SM traffic snooping.

```
Device(config)# ip pimsm-snooping
```

This example overrides the global setting and disable PIM SM traffic snooping on VLAN 20.

```
Device(config)# vlan 20
Device(config-vlan-20)# no ip pimsm-snooping
```

ip pim-sparse

Enables PIM Sparse on an interface that is connected to the PIM Sparse network.

Syntax

ip pim-sparse [**passive**]

no ip pim-sparse [**passive**]

Command Default

PIM Sparse is not enabled on the interface.

Parameters

passive

Specifies PIM passive mode on the interface.

Modes

Interface configuration mode

Usage Guidelines

The **no ip pim-sparse** command disables PIM Sparse.

The **no ip pim-sparse passive** command disables PIM passive mode on the interface.

You must enable PIM Sparse globally before you enable it on an interface.

If the interface is on the border of the PIM Sparse domain, you also must configure the **ip pim border** command.

Examples

This example adds an IP interface to port 1/2/2, then enable PIM Sparse on the interface.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e10000-2/2)# ip address 207.95.7.1 255.255.255.0
Device(config-if-e10000-2/2)# ip pim-sparse
```

ip policy route-map

Enables policy-based routing (PBR).

Syntax

ip policy route-map *map-name*

no ip policy route-map *map-name*

Command Default

PBR is not enabled.

Parameters

map-name

Specifies the name of the route map.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

This command can be used to enable PBR globally on all interfaces or on a specific interface.

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

Examples

The following example enables PBR globally.

```
device(config)# route-map map1
device(config-routemap map1)# exit
device(config)# ip policy route-map map1
```

The following example enables PBR on a specific interface.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ip policy route-map map1
```

ip preserve-acl-user-input-format

Preserves the user input format for ACL configuration.

Syntax

ip preserve-acl-user-input-format

no ip preserve-acl-user-input-format

Command Default

ACL implementations automatically display the TCP or UDP port name instead of the port number.

Modes

Global configuration mode

Usage Guidelines

When the option to preserve user input is enabled, the system displays either the port name or the number as used during configuration.

The **no** form of the command removes the user input perseverance configuration.

Examples

The following example shows the behavior when the option to preserve user input is enabled. In this example, the TCP port is configured by number (80) when configuring ACL group 140. However, **show ip access-lists 140** reverts to the port name for the TCP port (HTTP in this example). When the **ip preserve-acl-user-input-format** command is configured, the **show ip access-lists** command displays either the TCP port number or name, depending on how it was configured by the user.

```
device(config)# access-list 140 permit tcp any any eq 80
device(config)# access-list 140 permit tcp any any eq ftp
device(config)# exit

device# show ip access-lists 140
Extended IP access list 140
permit tcp any any eq http
permit tcp any any eq ftp

device(config)# access-list 140 permit tcp any any eq 80
device(config)# access-list 140 permit tcp any any eq ftp

device# show ip access-lists 140
Extended IP access list 140
permit tcp any any eq http
permit tcp any any eq ftp

device(config)# ip preserve-acl-user-input-format
device(config)# exit

device# show ip access-lists 140
Extended IP access list 140
permit tcp any any eq 80
permit tcp any any eq ftp
```

ip-proto

Configures an IP protocol-based VLAN.

Syntax

ip-proto [**name** *string*]

no ip-proto [**name** *string*]

Command Default

An IP protocol-based VLAN is not configured.

Parameters

name *string*

Specifies the name of the IP protocol VLAN. The maximum length of the string is 32 characters.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command removes the IP protocol-based VLAN.

Examples

The following example configures the IP protocol-based VLAN.

```
device (config)# vlan 10
device(config-vlan-10)# ip-proto name IP_Prot_VLAN
```

ip radius source-interface

Configures an interface as the source IP address from (using) which the RADIUS client sends RADIUS requests or receives responses.

Syntax

ip radius source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

no ip radius source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

Command Default

When the management VRF is configured, the RADIUS client sends RADIUS requests or receives responses only through the ports belonging to the management VRF and through the out-of-band management port.

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet interface address used for setting the source IP address.

loopback *number*

Specifies the loopback interface address used for setting the source IP address.

management *number*

Specifies the management interface address used for setting the source IP address.

ve *number*

Specifies the Virtual Ethernet interface address used for setting the source IP address.

Modes

Global configuration mode

Usage Guidelines

When a source interface is configured, management applications use the lowest configured IP address of the specified interface as the source IP address in all the outgoing packets. If the configured interface is not part of the management VRF, the response packet does not reach the destination.

The RADIUS source interface configuration command **ip radius source-interface** should be compatible with the management VRF configuration.

NOTE

Any change in the management VRF configuration takes effect immediately for the RADIUS client.

The **no** form of the command removes the configured interface as the source IP address for the RADIUS client.

Examples

The following example shows how to configure an Ethernet interface as the source IP address for the RADIUS client to send RADIUS requests or receive RADIUS responses.

```
device(config)# ip radius source-interface ethernet 1/1/1
```

The following example shows how to configure a loopback interface as the source IP address for the RADIUS client to send RADIUS requests or receive RADIUS responses.

```
device(config)# ip radius source-interface loopback 1
```

ip router-id

Configures IPv4 router ID.

Syntax

ip router-id *ipv4-address*

no ip router-id *ipv4-address*

Command Default

Router ID is not configured.

Parameters

ipv4-address

Specifies the IPv4 address. The default is the lowest IP in use.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the configured IPv4 router ID.

Examples

The following example shows how to configure the IPv4 router ID.

```
device(config)# ip router-id 10.14.52.11
```

ip show-portname

Displays interface names in Syslog messages.

Syntax

ip show-portname

no ip show-portname

Command Default

An interface slot number (if applicable) and port numbert along with the interface type are displayed when you display Syslog messages.

Modes

Global configuration mode

Usage Guidelines

Syslog messages show the interface type, such as "ethernet", and so on. However, if the**ip show-portname** command is configured and a name has been assigned to the port, the port name replaces the interface type.

The **no** form of the command displays the interface slot number and port number in Syslog messages.

Examples

The following example shows how to display the name of the interface.

```
device(config)# ip show-portname
```

ip show-service-number-in-log

Displays TCP or UDP port numbers instead of the port names.

Syntax

ip show-service-number-in-log

no ip show-service-number-in-log

Command Default

By default, the device displays TCP or UDP application information in named notation.

Modes

Global configuration mode

Usage Guidelines

When this command is enabled, the device will display http (the well-known port name) instead of 80 (the port number) in the output of show commands, and other commands that contain application port information.

The **no** form of the command displays TCP or UDP port name.

Examples

The following example shows how to set the display of TCP or UDP port numbers instead of their names.

```
device(config)# ip show-service-number-in-log
```

ip ssh authentication-retries

Configures the number of SSH authentication retries.

Syntax

ip ssh authentication-retries *number-retries*

no ip ssh authentication-retries *number-retries*

Command Default

By default, the Brocade device attempts to negotiate a connection with the connecting host three times.

Parameters

number-retries

The number of SSH authentication retries. Valid values are from 1 through 5.

Modes

Global configuration mode

Usage Guidelines

The **ip ssh authentication-retries** command is not applicable on devices that act as an SSH client. On such devices, when you try to establish an SSH connection with the wrong credentials, the session is not established and the connection is terminated. The device does not check the SSH authentication retry configuration set using the **ip ssh authentication-retries** command. The command is applicable only to SSH clients such as PuTTY, SecureCRT, and so on.

The **no** form of the command sets the number of retries to the default value of three.

Examples

The following example shows how to set the authentication retries to 5.

```
device(config)# ip ssh authentication-retries 5
```

ip ssh client

Restricts Secure Shell (SSH) access to a Brocade device based on the client IP address and MAC address.

Syntax

ip ssh client { *ipv4-address* [*mac-address*] | **any** *mac-address* | **ipv6** *ipv6-address* }

no ip ssh client { *ipv4-address* [*mac-address*] | **any** *mac-address* | **ipv6** *ipv6-address* }

Command Default

SSH access is not enabled.

Parameters

ipv4-address
: Allows SSH access from the host with the specified IP address.

mac-address
: Allows SSH access from the host with the specified IP address and MAC address.

any *mac-address*
: Allows SSH access from any host with any IP address and specified MAC address.

ipv6 *ipv6-address*
: Allows SSH access from any host with the specified IPv6 address.

Modes

Global configuration mode

Usage Guidelines

You can specify only one IP address with one command. However, you can enter the command ten times to specify up to ten IP addresses.

The **no** form of the command removes the SSH access restrictions.

Examples

The following example shows how to allow SSH access to a Brocade device based on the host with IP address 10.157.22.39.

```
device(config)# ip ssh client 10.157.22.39
```

The following example shows how to allow SSH access to the Brocade device based on the host with IP address 10.157.22.39 and MAC address 0000.000f.e9a0.

```
device(config)# ip ssh client 10.157.22.39 0000.000f.e9a0
```

The following example shows how to allow SSH access to the Brocade device based on the host with IPv6 address 2001::1 and MAC address 0000.000f.e9a0.

```
device(config)# ip ssh client ipv6 2001::1
```

ip ssh encryption aes-only

Enables SSH AES encryption and disables support for 3des-cbc.

Syntax

ip ssh encryption aes-only

no ip ssh encryption aes-only

Command Default

The 3des-cbc encryption is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the AES encryption support.

Examples

The following example shows how to enable AES encyrption.

```
device(config)# ip ssh encryption aes-only.
```

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(config)#  ip ssh encryption disable-aes-cbc
```

History

Release version	Command history
08.0.20a	This command was introduced.

ip ssh idle-time

Configures the amount of time an SSH session can be inactive before the device closes it.

Syntax

ip ssh idle-time *time*

no ip ssh idle-time *time*

Command Default

By default, SSH sessions do not time out.

Parameters

time

Time in minutes. Valid values are from 0 through 240. The default is 0 (never time out).

Modes

Global configuration mode

Usage Guidelines

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

If an established SSH session has no activity for the specified number of minutes, the device closes it. An idle time of 0 minutes (the default value) means that SSH sessions never time out.

Examples

The following example configures the SSH idle time to 50 minutes.

```
device(config)# ip ssh idle-time 50
```

ip ssh interactive-authentication

Configures the keyboard-interactive authentication.

Syntax

ip ssh interactive-authentication { **yes** | **no** }

no ip ssh interactive-authentication { **yes** | **no** }

Command Default

Keyboard-interactive authentication is not enabled.

Parameters

yes

Enables keyboard-interactive authentication.

no

Disables keyboard-interactive authentication.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables keyboard-interactive authentication.

Examples

The following example enables keyboard-interactive authentication.

```
device(config)# ip ssh interactive-authentication yes
```

ip ssh key-authentication

Configures DSA or RSA challenge-response authentication.

Syntax

ip ssh key-authentication { **yes** | **no** }

no ip ssh key-authentication { **yes** | **no** }

Command Default

DSA or RSA challenge-response authentication is enabled by default.

Parameters

yes

Enables DSA or RSA challenge-response authentication. The default is **yes**.

no

Disables DSA or RSA challenge-response authentication.

Modes

Global configuration mode

Usage Guidelines

After the SSH server on the Brocade device negotiates a session key and encryption method with the connecting client, user authentication takes place. The implementation of SSH supports DSA or RSA challenge-response authentication and password authentication. You can deactivate one or both user authentication methods for SSH. Note that deactivating both authentication methods disables the SSH server entirely.

With DSA or RSA challenge-response authentication, a collection of clients' public keys are stored on the device. Clients are authenticated using these stored public keys. Only clients that have a private key that corresponds to one of the stored public keys can gain access to the device using SSH.

The **no** form of the command disables DSA or RSA challenge-response authentication.

Examples

The following example enables DSA or RSA challenge-response authentication.

```
device(config)# ip ssh key-authentication
```

ip ssh key-exchange-method dh-group14-sha1

Configures diffie-hellman-group14-sha1 as the key-exchange method to establish an SSH connection.

Syntax

ip ssh key-exchange-method dh-group14-sha1

no ip ssh key-exchange-method dh-group14-sha1

Command Default

The diffie-hellman-group1-sha1 is used as the key-exchange method.

Modes

Global configuration mode

Usage Guidelines

The diffie-hellman-group14-sha1 key-exchange method is supported only on Brocade FCX device.

The **ip ssh key-exchange-method dh-group14-sha1** command is not supported in FIPS or CC mode.

In FIPS mode, only diffie-helman-group-exchange-sha256 is supported and in common criteria(CC) mode, only diffie-hellman-group14-sha1 is supported.

The **no** form of the command restores diffie-hellman-group1-sha1 as the key-exchange method.

Examples

The following example overrides the default key-exchange method and configures diffie-hellman-group14-sha1 as the key-exchange method.

```
device(config)# ip ssh  key-exchange-method dh-group14-sha1
```

History

Release version	Command history
08.0.30f	This command was introduced.

ip ssh password-authentication

Configures password authentication.

Syntax

ip ssh password-authentication { **yes** | **no** }

no ip ssh password-authentication { **yes** | **no** }

Command Default

Password authentication is enabled.

Parameters

yes

Enables the password authentication. The default is **yes**.

no

Disables the password authentication.

Modes

Global configuration mode

Usage Guidelines

After the SSH server on the device negotiates a session key and encryption method with the connecting client, user authentication takes place. The implementation of SSH supports DSA or RSA challenge-response authentication and password authentication. You can deactivate one or both user authentication methods for SSH. Note that deactivating both authentication methods disables the SSH server entirely.

With password authentication, users are prompted for a password when they attempt to log in to the device (provided empty password logins are not allowed). If there is no user account that matches the username and password supplied by the user, the user is not granted access.

The **no** form of the command enables password authentication.

Examples

The following example disables the password authentication.

```
device(config)# ip ssh password-authentication yes
```

ip ssh permit-empty-password

Allows a user with an SSH client to log in without being prompted for a password.

Syntax

ip ssh permit-empty-password { **yes** | **no** }

no ip ssh permit-empty-password { **yes** | **no** }

Command Default

By default, empty password logins are not allowed.

Parameters

yes

Allows a user to log in to an SSH client without being prompted for a password.

no

Disallows a user to log in to an SSH client without being prompted for a password.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disallows user to log in without being prompted for a password.

By default, empty password logins are not allowed; users with an SSH client are always prompted for a password when they log in to the device. To gain access to the device, each user must have a username and password. Without a username and password, a user is not granted access.

If you enable empty password logins, users are not prompted for a password when they log in. Any user with an SSH client can log in without being prompted for a password.

Examples

The following example enables the user to log in to an SSH client without being prompted for a password.

```
device(config)# ip ssh permit-empty-password yes
```

ip ssh port

Configures the port for SSH traffic.

Syntax

ip ssh port *port-num*

no ip ssh port *port-num*

Command Default

By default, SSH traffic occurs on TCP port 22.

Parameters

port-num

Specifies the port number.

Modes

Global configuration mode

Usage Guidelines

If you change the default SSH port number, you must configure SSH clients to connect to the new port. Also, you should be careful not to assign SSH to a port that is used by another service. If you change the SSH port number, Brocade recommends that you change it to a port number greater than 1024.

The **no** form of the command changes the port to the default.

Examples

The following example configures the SSH port as 2200.

```
device(config)# ip ssh port 2200
```

ip ssh pub-key-file

Imports the authorized public keys into the active configuration of the device by loading the public key file from a TFTP server.

Syntax

ip ssh pub-key-file { **remove** | **tftp** { *ipv4-address* | **ipv6** *ipv6-address*} *file-name* }

no ip ssh pub-key-file { **remove** | **tftp** { *ipv4-address* | **ipv6** *ipv6-address*} *file-name* }

Command Default

The private key is normally stored in a password-protected file on the local host; the public key is stored in another file and is not protected.

Parameters

remove
Removes the SSH client public key file from the device.

tftp
Imports DSS public key from the TFTP server.

ipv4-address
Specifies the IPv4 address of the TFTP server.

ipv6 *ipv6-address*
Specifies the IPv6 address of the TFTP server.

file-name
Specifies the public key file name.

Modes

Global configuration mode

Usage Guidelines

You can use the **show ip client-pub-key** command to display the currently loaded public keys.

SSH clients that support DSA or RSA authentication normally provide a utility to generate a DSA or RSA key pair. The private key is normally stored in a password-protected file on the local host; the public key is stored in another file and is not protected. You must import the client public key for each client into the Brocade device.

The **no** form of the command removes the imported public keys.

Examples

The following example imports a public key file from the TFTP server 192.168.10.1.

```
device(conig)# ip ssh pub-key-file tftp 192.168.10.1 pkeys.txt
```

The following example removes a public key file from the device.

```
device(confg)# ip ssh pub-key-file remove
```

ip ssh scp

Enables Secure Copy (SCP).

Syntax

ip ssh scp { **enable** | **disable** }

no ip ssh scp { **enable** | **disable** }

Command Default

SCP is enabled.

Parameters

enable

Enables SCP.

disable

Disables SCP.

Modes

Global configuration mode

Usage Guidelines

SCP uses security built into SSH to transfer image and configuration files to and from the device. SCP automatically uses the authentication methods, encryption algorithm, and data compression level configured for SSH.

If you disable SSH, SCP is also disabled.

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

Examples

The following example disables SCP.

```
device(config)# ip ssh scp disable
```

The following example enables SCP.

```
device(config)# ip ssh scp enable
```

ip ssh strict-management-vrf

Allows the incoming SSH connection requests only from the management VRF and not from the out-of-band management port.

Syntax

ip ssh strict-management-vrf

no ip ssh strict-management-vrf

Command Default

When the management VRF is configured, the incoming SSH connection requests are allowed from the ports belonging to the management VRF and from the out-of-band management port.

Modes

Global configuration mode

Usage Guidelines

The **ip ssh strict-management-vrf** command is applicable only when the management VRF is configured. If management VRF is not configured, configuring the **ip ssh strict-management-vrf** command displays a warning message.

For the SSH server, changing the management VRF configuration or configuring the **ip ssh strict-management-vrf** command does not affect the existing SSH connections. The changes are applied only to the new incoming connection requests.

The **no** form of the command enables the incoming SSH connection requests from the ports belonging to the management VRF and from the out-of-band management port.

Examples

The following example shows how to configure the incoming SSH connection requests from the management VRF only.

```
device(config)# ip ssh strict-management-vrf
```

ip ssh timeout

Configures the wait time for a response from the client when the SSH server attempts to negotiate a session key and encryption method with a connecting client.

Syntax

ip ssh timeout *time*

no ip ssh timeout *time*

Command Default

The default timeout value is 120 seconds.

Parameters

time

Timeout value in seconds. The valid range is from 1 through 120 seconds.

Modes

Global configuration mode

Usage Guidelines

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

Examples

The following example configures the SSH timeout value to 60 seconds.

```
device(config)# ip ssh timeout 60
```

ip ssl

Configures Secure Socket Layer (SSL) settings.

Syntax

ip ssl cert-key-size *size*

no ip ssl cert-key-size *size*

ip ssl { **certificate-data-file** | **client-certificate** | **client-private-key** | **private-key-file** } **tftp** { *ipv4-address* | **ipv6** *ipv6-address*} *file-name*

no ip ssl { **certificate-data-file** | **client-certificate** | **client-private-key** | **private-key-file** } **tftp** { *ipv4-address* | **ipv6** *ipv6-address*} *file-name*

ip ssl port *port-num*

no ip ssl port *port-num*

ip ssl certificate { **common-name** | **country** | **locality** | **org** | **org-unit** | **state** } *name*

no ip ssl certificate { **common-name** | **country** | **locality** | **org** | **org-unit** | **state** } *name*

Command Default

The default key size for Brocade-issued and imported digital certificates is 2048 bits.

By default, SSL protocol exchanges occur on TCP port 443.

The default TFTP server is not configured.

Parameters

cert-key-size *size*
: Configures SSL server certificate key size. Valid values are 2048 and 4096.

certificate-data-file
: Imports the server RSA certificate.

client-certificate
: Imports the client RSA certificate.

client-private-key
: Imports the client RSA private key.

private-key-file
: Imports the server RSA private key.

tftp
: Specifies that TFTP is used to import the certificates.

ipv4-address
: Configures the IPv4 address of the TFTP server from which the certificates are imported.

ipv6 *ipv6-address*
: Configures the IPv6 address of the TFTP server from which the certificates are imported.

file-name
: The certificate data file name.

port *port-num*
Specifies the HTTPS/SSL port. The default port is 443.

certificate
Configures the SSL certificate generation signing request.

common-name
Specifies the common name, fully qualified domain name, or web address for which you plan to use your certificate.

country
Specifies the country name.

locality
Specifies the locality name.

org
Specifies the organization name.

org-unit
Specifies the organization unit name.

state
Specifies the state or province name.

name
Fully qualified domain name or web address for which you plan to use your certificate (for example, www.server.com) when used with **common-name**, two letter code country name (for example, US) when used with **country**, locality name (for example, city) when used with **locality**, organization name (for example, company) when used with **org**, organization unit name (for example, section) when used with **org-unit**, or province name (for example, California) when used with **state**.

Modes

Global configuration mode

Usage Guidelines

The SSL server certificate key size applies only to digital certificates issued by Brocade and does not apply to imported certificates.

To allow a client to communicate with another Brocade device using an SSL connection, you configure a set of digital certificates and RSA public-private key pairs on the device. A digital certificate is used for identifying the connecting client to the server. It contains information about the issuing Certificate Authority CA), as well as a public key. You can either import digital certificates and private keys from a server, or you can allow the Brocade device to create them. The RSA private key can be up to 4096 bits.

The **no** form of the command removes the configurations.

Examples

The following example shows how to import a digital certificate issued by a third-party Certificate Authority (CA) and save it in the flash memory.

```
device(config)# ip ssl certificate-data-file tftp 10.10.10.1 cacert.pem
```

The following example shows how to change the key size for Brocade-issued and imported digital certificates to 4096 bits.

```
device(config)# ip ssl cert-key-size 4096
```

The following example shows how to change the port number used for SSL communication.

```
device(config)# ip ssl port 334
```

The following example shows how to import an RSA private key from a client.

```
device(config)# ip ssl private-key-file tftp 192.168.9.210 keyfile
```

The following example shows how to configure the SSL certificate generation signing request for a country.

```
device(config)# ip ssl certificate country us
```

ip ssl min-version

Configures the minimum TLS version to be used to establish the TLS connection.

Syntax

ip ssl min-version { **tls_1_0** | **tls_1_1** | **tls_1_2** }

no ip ssl min-version { **tls_1_0** | **tls_1_1** | **tls_1_2** }

Command Default

For devices which act as an SSL server or HTTPS server, the default connection is with TLS1.2.

For the Brocade device which acts as the SSL client or the syslog, OpenFlow, or secure AAA client, the TLS version is decided based on the server support.

Parameters

tls_1_0
: Specifies TLS 1.0 as the minimum version.

tls_1_1
: Specifies TLS 1.1 as the minimum version.

tls_1_2
: Specifies TLS 1.2 as the minimum version.

Modes

Global configuration mode

Usage Guidelines

If **tls_1_1** is set as the minimum version, TLS 1.1 and later versions are supported.

The **no** form of the command removes the minimum TLS version configuration and supports all TLS versions.

Examples

The following example establishes the TLS connection using the TLS 1.1 version and above.

```
device(config)# ip ssl min-version tls_1_1
```

History

Release version	Command history
08.0.20a	This command was introduced.

ip-subnet

Configures an IP subnet VLAN within a VLAN.

Syntax

ip-subnet { *ip-address ip-mask* [**name** *string*] }

no ip-subnet { *ip-address ip-mask* [**name** *string*] }

Command Default

A VLAN is not configured with an IP subnet and mask.

Parameters

ip-address

Specifies the IP address you want to assign to a VLAN. The IP address can be in the format A.B.C.D or A.B.C.D/L, where L is the subnet mask length.

ip-mask

Specifies the subnet mask you want to assign. This is required when the subnet mask length is not specified along with the IP address.

name *string*

Specifies the name of the IP subnet. The name can be up to 32 characters in length.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command removes the IP subnet VLAN.

Examples

The following example shows how to configure an IP subnet VLAN within a VLAN.

```
device(config)# vlan 4
device(config-vlan-4)# ip-subnet 10.1.3.0/24 name Brown
```

ip syslog source-interface

Configures an interface as the source IP address from (using) which the Syslog module sends log messages.

Syntax

ip syslog source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

no ip syslog source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

Command Default

When the management VRF is configured, the Syslog module sends log messages only through the ports belonging to the management VRF and the out-of-band management port.

Parameters

ethernet *stackid/slot/port*
Specifies the Ethernet interface address to be used as the source IP address.

loopback *number*
Specifies the loopback interface to be used as the source IP address.

management *number*
Specifies the management interface to be used as the source IP address.

ve *number*
Specifies the Virtual Ethernet interface to be used as the source IP address.

Modes

Global configuration mode

Usage Guidelines

When a source interface is configured, management applications use the lowest configured IP address of the specified interface as the source IP address in all the outgoing packets. If the configured interface is not part of the management VRF, the response packet does not reach the destination.

The Syslog source interface configuration command **ip syslog source-interface** should be compatible with the management VRF configuration. Any change in the management VRF configuration takes effect immediately for Syslog.

The **no** form of the command removes the configured interface as the source IP address.

Examples

The following example shows how to configure an ethernet interface as the source IP address for the Syslog module to send log messages.

```
device(config)# ip syslog source-interface ethernet 1/1/1
```

The following example shows how to configure a management interface as the source IP address for the Syslog module to send log messages.

```
device(config)# ip syslog source-interface management 1
```

ip tacacs source-interface

Configures an interface as the source IP address from (using) which the TACACS+ client establishes connections with TACACS+ servers.

Syntax

ip tacacs source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

no ip tacacs source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

Command Default

TACACS+ source interface is not configured.

When the management VRF is configured, the TACACS+ client establishes connections with TACACS+ servers only through the ports belonging to the management VRF and the out-of-band management port.

Parameters

ethernet *stackid/slot/port*
Specifies the Ethernet interface to be used as the source IP address.

loopback *number*
Specifies the loopback interface to be used as the source IP address.

management *number*
Specifies the management interface to be used as the source IP address.

ve *number*
Specifies the Virtual Ethernet interface to be used as the source IP address.

Modes

Global configuration mode

Usage Guidelines

For the TACACS+ client, a change in the management VRF configuration does not affect the existing TACACS+ connections. The changes are applied only to new TACACS+ connections.

The TACACS+ source interface configuration command **ip tacacs source-interface** must be compatible with the management VRF configuration.

The **no** form of the command removes the configured interface as the source IP address.

Examples

The following example shows how to configure an Ethernet interface as the source IP address for the TACACS+ client to establish connections with TACACS+ servers.

```
device(config)# ip tacacs source-interface ethernet 1/1/1
```

The following example shows how to configure a Virtual Ethernet interface as the source IP address for the TACACS+ client to establish connections with TACACS+ servers.

```
device(config)# ip tacacs source-interface ve 1
```

ip tcp burst-normal

Configures the threshold values for TCP SYN packets that are targeted at the router itself or passing through an interface.

Syntax

ip tcp burst-normal *num-packets* **burst-max** *num-packets* **lockup** *time*

no ip tcp burst-normal *num-packets* **burst-max** *num-packets* **lockup** *time*

Command Default

The threshold value is not configured.

Parameters

num-packets
: Configures the number of packets per second in normal burst mode. Valid values are from 1 through 100,000 packets per second.

burst-max *num-packets*
: Specifies the number of packets per second in maximum burst mode. Valid values are from 1 through 100,000 packets per second.

lockup *time*
: Configures the lockup period in seconds. Valid values are from 1 through 10,000 seconds.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

In a TCP SYN attack, an attacker floods a host with TCP SYN packets that have random source IP addresses. For each of these TCP SYN packets, the destination host responds with a SYN ACK packet and adds information to the connection queue. However, because the source host does not exist, no ACK packet is sent back to the destination host, and an entry remains in the connection queue until it ages out (after approximately one minute). If the attacker sends enough TCP SYN packets, the connection queue can fill up, and service can be denied to legitimate TCP connections.

To protect against TCP SYN attacks, you can configure the Brocade device to drop TCP SYN packets when excessive number of packets are encountered. You can set threshold values for TCP SYN packets that are targeted at the router itself or passing through an interface, and drop them when the thresholds are exceeded.

For Layer 3 router code, if the interface is part of a VLAN that has a router VE, you must configure TCP SYN attack protection at the VE level. When TCP SYN attack protection is configured at the VE level, it will apply to routed traffic only. It will not affect switched traffic.

NOTE
You must configure VLAN information for the port before configuring TCP SYN attack protection. You cannot change the VLAN configuration for a port on which TCP SYN attack protection is enabled.

NOTE
This command is available at the global configuration level on both chassis devices and compact devices. On chassis devices, this command is available at the interface level as well. This command is supported on Ethernet and Layer 3 interfaces.

The number of incoming TCP SYN packets per second is measured and compared to the threshold values as follows:

- If the number of TCP SYN packets exceeds the **burst-normal** value, the excess TCP SYN packets are dropped.
- If the number of TCP SYN packets exceeds the **burst-max** value, all TCP SYN packets are dropped for the number of seconds specified by the **lockup** value. When the lockup period expires, the packet counter is reset and measurement is restarted.

The **no** form of the command removes the threshold value set for TCP SYN packets.

Examples

The following example sets the threshold value for TCP SYN packets targeted at the router.

```
device(config)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

The following example sets the threshold value for TCP SYN packets received on interface 1/1/1.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

The following example sets the threshold value for TCP SYN packets received on VE 31.

```
device(config)# interface ve 31
device(config-vif-31)# ip tcp burst-normal 5000 burst-max 10000 lockup 300
```

ip tcp keepalive

Configures the time interval between TCP keepalive messages.

Syntax

ip tcp keepalive *timeout interval-time num-messages*

no ip tcp keepalive *timeout interval-time num-messages*

Command Default

The time interval between TCP keepalive messages is not configured.

Parameters

timeout

Configures the timeout in seconds to start sending keepalive messages. Set to 0 to disable the timeout.

interval-time

Configures the interval time in seconds between keepalive messages. Set to 0 to disable sending keepalive messages.

num-messages

Configures the number of keepalive messages to be sent before disconnecting.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables sending the keepalive messages. You can also set the *interval-time* variable as 0 to disable sending the keepalive messages.

Examples

The following example configures the interval between TCP keepalive messages as 5 seconds.

```
device(config)# ip tcp keepalive 10 5 2
```

ip tftp source-interface

Configures an interface as the source IP address from (using) which the TFTP sends or receives data and acknowledgments.

Syntax

ip tftp source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

no ip tftp source-interface { **ethernet** *stackid/slot/port* | **loopback** *number* | **management** *number* | **ve** *number* }

Command Default

TFTP source interface is not configured.

When the management VRF is configured, TFTP sends or receives data and acknowledgments only through ports belonging to the management VRF and through the out-of-band management port.

Parameters

ethernet *stackid/slot/port*
Specifies the Ethernet interface to be used as the source IP address.

loopback *number*
Specifies the loopback interface to be used as the source IP address.

management *number*
Specifies the management interface to be used as the source IP address.

ve *number*
Specifies the Virtual Ethernet interface to be used as the source IP address.

Modes

Global configuration mode

Usage Guidelines

Any change in the management VRF configuration takes effect immediately for TFTP. You cannot make changes in the management VRF configuration while TFTP is in progress.

The TFTP source interface configuration command **ip tftp source-interface** should be compatible with the management VRF configuration.

The **no** form of the command removes the configured ethernet/loopback/management/ve interface as the source IP address.

Examples

The following example shows how to configure an Ethernet interface as the source IP address for the TFTP to send or receive data and acknowledgments.

```
device(config)# ip tftp source-interface ethernet 1/1/1
```

The following example shows how to configure a loopback interface as the source IP address for the TFTP to send or receive data and acknowledgments.

```
device(config)# ip tftp source-interface loopback 1
```

ip use-acl-on-arp

Configures the ARP module to check the source IP address of the ARP request packets received on the interface before applying the specified ACL policies to the packet (ACL ARP filtering).

Syntax

ip use-acl-on-arp [*acl-num*]

no ip use-acl-on-arp [*acl-num*]

Command Default

ACL ARP filtering is not enabled.

Parameters

acl-num

Specifies an ACL number to explicitly specify the ACL to be used for filtering.

Modes

Interface configuration mode

Usage Guidelines

ACL ARP filtering is not applicable to outbound traffic.

This command is available on devices running Layer 3 code. This filtering occurs on the management processor. The command is available on physical interfaces and virtual routing interfaces. ACLs used to filter ARP packets on a virtual routing interface can be inherited from a previous interface if the virtual routing interface is defined as a follower virtual routing interface. Only extended ACLs that use IP only can be used. If any other ACL is used, an error is displayed.

When the **ip use-acl-on-arp** command is configured, the ARP module checks the source IP address of the ARP request packets received on the interface. It then applies the specified ACL policies to the packet. Only the packet with the IP address that the ACL permits will be allowed to be written in the ARP table; those that are not permitted will be dropped.

ARP requests will not be filtered by ACLs if one of the following conditions occur:

- If the ACL is to be inherited from an IP ACL, but there is no IP ACL defined.
- An ACL ID is specified for the **ip use-ACL-on-arp** command, but no IP address or "any any" filtering criteria has been defined under the ACL ID.

The **no** form of the command disables the ACL ARP filtering.

Examples

The following example shows a complete ACL ARP configuration.

```
device(config)# access-list 101 permit ip host 192.168.2.2 any
device(config)# access-list 102 permit ip host 192.168.2.3 any
device(config)# access-list 103 permit ip host 192.168.2.4 any
device(config)# vlan 2
device(config-vlan-2)# tag ethernet 1/1/1 to 1/1/2
device(config-vlan-2)# router-interface ve 2
device(config-vlan-2)# vlan 3
device(config-vlan-3)# tag ethernet 1/1/1 to 1/1/2
device(config-vlan-3)# router-int ve 3
device(config-vlan-3)# vlan 4
device(config-vlan-4)# tag ethernet 1/1/1 to 1/1/2
device(config-vlan-4)# router-int ve 4
device(config-vlan-4)# interface ve 2
device(config-ve-2)# ip access-group 101 in
device(config-ve-2)# ip address 192.168.2.1/24
device(config-ve-2)# ip use-acl-on-arp 103
device(config-ve-2)# exit
device(config)# interface ve 3
device(config-ve-3)# ip access-group 102 in
device(config-ve-3)# ip follow ve 2
device(config-ve-3)# ip use-acl-on-arp
device(config-ve-3)# exit
device(config-vlan-4)# interface ve 4
device(config-ve-4)# ip follow ve 2
device(config-ve-4)# ip use-acl-on-arp
device(config-ve-4)# exit
```

ipv6 access-list

Configures an IPv6 access list and enters IPv6 access list configuration mode.

Syntax

ipv6 access-list *acl-name*

no ipv6 access-list *acl-name*

Command Default

The IPv6 ACL is not configured.

Parameters

acl-name

The IPv6 access list name.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the configured IPv6 access list.

Examples

The following example configures an IPv6 access list named acl1.

```
device(config)# ipv6 access-list acl1
device(config-ipv6-access-list acl1)#
```

ipv6 address

Configures an IPv6 address for an interface.

Syntax

ipv6 address *ipv6-prefix* [**anycast** | **eui-64**]

no ipv6 address *ipv6-prefix* [**anycast** | **eui-64**]

ipv6 address *ipv6-address* **link-local**

no ipv6 address *ipv6-address* **link-local**

Command Default

IPv6 address is not configured.

Parameters

ipv6-prefix

Specifies the IPv6 Prefix address in the format X:X::X:X/M.

anycast

Configures address as anycast address.

eui-64

Configures the global address with an EUI-64 interface ID in the low-order 64 bits. The interface ID is automatically constructed in IEEE EUI-64 format using the interface's MAC address.

ipv6-address

Specifies the IPv6 address.

link-local

Configures the address as link-local address.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command removes the IPv6 address.

Examples

The following example configures IPv6 address for the tunnel interface.

```
device(config)# interface tunnel 1
device(config-tnif-1)# ipv6 address 2001:DB8:384d:34::/64 eui-64
```

ipv6 cache-lifetime

Configures the IPv6 cache-aging lifetime.

Syntax

ipv6 cache-lifetime *interval*

no ipv6 cache-lifetime *interval*

Command Default

Cache aging is enabled except on the Ruckus ICX 7750.

Parameters

interval

Specifies the cache timeout interval in seconds. The default is 300 seconds.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of this command disables cache aging.

On the Ruckus ICX 7750, cache aging is disabled by default. You must ... to enable it.

Examples

This example sets the cache-aging interval to 17 seconds.

```
Device (config)# ipv6 cache-lifetime 17
```

History

Release version	Command history
8.0.30	This command was introduced.

ipv6 dhcp-relay destination

Enables the IPv6 DHCP relay agent function and specifies the IPv6 address as a destination address to which the client messages are forwarded.

Syntax

ipv6 dhcp-relay destination *ipv6-address*

no ipv6 dhcp-relay destination *ipv6-address*

Command Default

The IPv6 DHCP relay agent function is disabled.

Parameters

ipv6-address

Specifies the IPv6 address as a destination address to which the client messages can be forwarded.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command removes the DHCP relay agent from the interface.

You can configure up to 16 relay destination addresses on an interface.

Examples

The following example enables the DHCPv6 relay agent function and specifies the relay destination (the DHCP server) address on an interface.

```
device(config)# interface ethernet 2/3
device(config-if-e10000-2/3)# ipv6 dhcp-relay destination 2001::2
device(config-if-e10000-2/3)# ipv6 dhcp-relay destination fe80::224:38ff:febb:e3c0
outgoing-interface ethernet 2/5
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

ipv6 dhcp-relay distance

Assigns the administrative distance to IPv6 DHCP static routes installed in the IPv6 route table for the delegated prefixes on the interface.

Syntax

ipv6 dhcp-relay distance *value*

no ipv6 dhcp-relay distance *value*

Command Default

The administrative distance is not assigned.

Parameters

value

Assigns the administrative distance to DHCPv6 static routes on the interface. The range is from 1 through 255. If the value is set to 255, then the delegated prefixes for this interface will not be installed in the IPv6 static route table.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command sets the parameter to a default value of 10.

The administrative distance value must be set so that it does not replace the same IPv6 static route configured by the user.

Examples

The following example sets the administrative distance value to 25.

```
device(config-if-eth2/1)# ipv6 dhcp-relay distance 25
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

ipv6 dhcp-relay include-options

Includes the parameters on the IPv6 DHCP relay agent messages.

Syntax

ipv6 dhcp-relay include-options *interface-id*

no ipv6 dhcp-relay include-options *interface-id*

Command Default

The interface-ID parameter is 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.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables the relay agent include options parameters.

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.

Examples

The following example includes the interface-ID parameter on the DHCPv6 relay agent messages.

```
device(config)# interface ethernet 1/1/3
device(config-if-eth1/1/3)# ipv6 dhcp-relay include-options interface-id
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

ipv6 dhcp-relay maximum-delegated-prefixes

Sets the number of delegated prefixes that can be learned at the global and interface levels.

Syntax

ipv6 dhcp-relay maximum-delegated-prefixes *value*

no ipv6 dhcp-relay maximum-delegated-prefixes *value*

Command Default

The DHCPv6 Relay Agent Prefix Delegation Notification is enabled when the DHCPv6 relay agent feature is enabled on the interface.

Parameters

value

Limits the maximum number of prefixes that can be learned at the global level. The range is from 0 through 512. The global level default value is 500 while the interface level default is 100.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of the command sets the parameter to the default value of the specified platform.

You can disable the DHCPv6 Relay Agent Prefix Delegation Notification at the system or the interface level by setting ipv6 dhcp-relay maximum-delegated prefixes to 0 at the system or interface level.

The sum of all the delegated prefixes that can be learned at the interface level is limited by the system maximum. Make sure that there is enough free space in the flash memory to save information about delegated prefixes in flash on both the active and standby management processors.

Examples

The following example sets the maximum delegated prefixes to 500 at the global level.

```
device(config)# ipv6 dhcp-relay maximum-delegated-prefixes 500
```

The following example sets the maximum delegated prefixes to 100 at the interface level.

```
device(config)# config-if-eth2/1
device(config-if-eth2/1)# ipv6 dhcp-relay maximum-delegated-prefixes 100
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

ipv6 dhcp6 snooping

Enables DHCPv6 snooping on a VLAN.

Syntax

ipv6 dhcp6 snooping *vlan id*

no ipv6 dhcp6 snooping *vlan id*

Command Default

DHCPv6 snooping is disabled by default.

Parameters

vlan id

Specifies the ID of a configured client or DHCPv6 server VLAN.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command disables DHCPv6 snooping on the VLAN.

DHCPv6 snooping must be enabled on the client and the DHCPv6 server VLANs.

Examples

The following example enables DHCPv6 snooping on VLAN 2.

```
device(config)# ipv6 dhcp6 snooping vlan 2
```

ipv6 enable

Enables IPv6.

Syntax

ipv6 enable

no ipv6 enable

Command Default

IPv6 is enabled by default in the Layer 2 switch code.

IPv6 is disabled by default in the router code.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

IPv6 is enabled by default in the Layer 2 switch code. If desired, you can disable IPv6 on a global basis on a device running the switch code.

IPv6 is disabled by default in the router code and must be configured on each interface that will support IPv6. In router code, the **ipv6 enable** command enables IPv6 on the switch and specifies that the interface is assigned an automatically computed link-local address

Before an IPv6 ACL can be applied to an interface, it must first be created, and then IPv6 must be enabled on that interface.

The **no** form of the command disables IPv6 on the interface.

Examples

The following example re-enables the IPv6 after it has been disabled.

```
device(config)# ipv6 enable
```

The following example enables IPv6 on Ethernet interface 1/1/1.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ipv6 enable
```

ipv6 hitless-route-purge-timer

Configures the timer to set the duration for which the routes should be preserved after switchover.

Syntax

ipv6 hitless-route-purge-timer *seconds*

no ipv6 hitless-route-purge-timer *seconds*

Command Default

The default timer setting is 45 seconds.

Parameters

seconds

Specifies the time after switchover to start IPv6 route purge. The value can range from 2 to 600 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the configured value and sets the timer to the default 45 seconds.

This command is supported only on the FastIron X Series devices (FSX 800 and FSX 1600).

Examples

The following example shows how to set the IPv6 hitless purge timer to 75 seconds.

```
device(config)# ipv6 hitless-route-purge-timer 60
```

ipv6 load-sharing

Enables ECMP load sharing for IPv6.

Syntax

ipv6 load-sharing [*num*]

no ipv6 load-sharing [*num*]

Command Default

ECMP load sharing for IPv6 is enabled and allows traffic to be balanced across up to four equal paths.

Parameters

num

Specifies the number of load sharing paths. The value can range from 2 to 8. The default value is 4.

Modes

Global configuration mode.

Usage Guidelines

If you want to re-enable the feature after disabling it, you must specify the number of load-sharing paths.

The **no** form of the command sets the load sharing path to the default value 4.

Examples

The following example sets the number of ECMP load sharing paths for IPv6 to 6.

```
device(config)# ipv6 load-sharing 6
```

ipv6 max-mroute

Configures the maximum number of IPv6 multicast routes that are supported.

Syntax

ipv6 max-mroute *num*

no ipv6 max-mroute *num*

Command Default

No maximum number of supported routes is configured.

Parameters

num

Configures the maximum number of multicast routes supported.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command restores the default (no maximum number of supported routes is configured).

Examples

The following example configures the maximum number of 20 supported IPv6 multicast routes on the VRF named my_vrf.

```
Device(config)# vrf my_vrf
Device(config)# address-family ipv6
Device(config-vrf)# ipv6 max-mroute 20
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mld group-membership-time

Specifies the multicast listener discovery (MLD) group membership time for the default VRF or for a specified VRF.

Syntax

ipv6 mld group-membership-time *num*

no ipv6 mld group-membership-time *num*

Command Default

An MLD group will remain active on an interface in the absence of a group report for 260 seconds, by default.

Parameters

num

Number in seconds, from 5 through 26000.

Modes

Global configuration mode.

VRF configuration mode.

Usage Guidelines

The **no** form of this command resets the group membership time interval to the default of 260 seconds.

Group membership time defines how long a group will remain active on an interface in the absence of a group report.

Examples

This example specifies an MLD group membership time of 2000 seconds for the default VRF.

```
device# configure terminal
device(config)# ipv6 mld group-membership-time 2000
```

This example specifies an MLD group membership time of 2000 seconds for a specified VRF.

```
device# configure terminal
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld group-membership-time 2000
```

ipv6 mld llqi

Configures the multicast listener discovery (MLD) last listener query interval.

Syntax

ipv6 mld llqi *seconds*

no ipv6 mld llqi *seconds*

Command Default

The MLD last listener query interval is 1 second.

Parameters

seconds

specifies the number in seconds, of MLD group addresses available for all VRFs. The range is 1 through 25; the default is 1.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of this command restores the default MLD last listener query interval.

Any MLD group memberships exceeding the group limit are not processed.

The last listener query interval is the maximum response delay inserted into multicast address-specific queries sent in response to Done messages, and is also the amount of time between multicast address-specific query messages. When a device receives an MLD Version 1 leave message or an MLD Version 2 state-change report, it sends out a query and expects a response within the time specified by the last listener query interval. Configuring a lower value for the last listener query interval allows members to leave groups faster.

Examples

This example configures a last listener query interval of 5 seconds.

```
Device(config)# ipv6 mld llqi 5
```

This example configures a last listener query interval of 5 seconds for a VRF.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# ipv6 mld llqi 5
```

ipv6 mld max-group-address

Configures the maximum number of MLD addresses for the default virtual routing and forwarding (VRF) instance or for a specified VRF.

Syntax

ipv6 mld max-group-address *num*

no ipv6 mld max-group-address *num*

Command Default

If this command is not configured, the maximum number of MLD addresses is determined by available system resources.

Parameters

num

specifies the maximum number of MLD group addresses available for all VRFs. The range is 1 through 8192; the default is 4096.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

If the **no** form of this command is configured, the maximum number of MLD addresses is determined by available system resources.

Any MLD group memberships exceeding the group limit are not processed.

Examples

This example configures a maximum of 1000 IGMP addresses for the default VRF.

```
Device(config)# ipv6 mld max-group-address 1000
```

This example configures a maximum of 1000 IGMP addresses for the VRF named vpn1.

```
Device(config)# vrf vpn1
Device(config-vrf-vpn1)# address-family ipv4
Device(config-vrf-vpn1-ipv4)# ip igmp max-group-address 1000
```

ipv6 mld max-response-time

Configures the maximum time a multicast listener has to respond to queries for the default virtual routing and forwarding (VRF) instance or for a specified VRF.

Syntax

ipv6 mld max-response-time *num*

no ipv6 mld max-response-time *num*

Command Default

If this command is not configured, the maximum time a multicast listener has to respond to queries is 10 seconds.

Parameters

num

specifies the maximum time, in seconds, a multicast listener has to respond. The range is 1 through 25; the default is 10.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

If the **no** form of this command is configured, the maximum time a multicast listener has to respond to queries is 10 seconds.

Examples

The following example configures the maximum time a multicast listener has to respond to queries to 20 seconds.

```
device# configure terminal
device(config)# ipv6 mld max-response-time 20
```

The following example configures the maximum time a multicast listener has to respond to queries to 20 seconds for the VRF named vpn1.

```
device# configure terminal
device(config)# vrf vpn1
Device(config-vrf-vpn1)# address-family ipv6
device(config)# ipv6 mld max-response-time 20
```

ipv6 mld port-version

Configures the multicast listening discovery (MLD) version on a virtual Ethernet interface.

Syntax

ipv6 mld port-version *version-number*

no ipv6 mld port-version

Command Default

The port uses the MLD version configured globally.

Parameters

version-number

Specifies the MLD version, 1 or 2.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the MLD version configured globally.

Examples

This example configures MLD version 2 on virtual Ethernet interface 10.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld port-version 2
```

ipv6 mld query-interval

Configures the frequency at which multicast listening discovery (MLD) query messages are sent.

Syntax

ipv6 mld query-interval *num*

no ipv6 mld query-interval *num*

Command Default

125 seconds

Parameters

num

Number in seconds, from 2 through 3600. The default is 125.

Modes

Global configuration mode.

VRF configuration mode.

Usage Guidelines

The **no** form of this command resets the query interval to the default of 125 seconds.

You must specify a query-interval value that is greater than the interval configured by the `ipv6 mld max-response-time` command.

Examples

This example sets the MLD query interval to 50 seconds.

```
Device(config)# ipv6 mld query-interval 50
```

This example sets the MLD query interval for a VRF to 50 seconds.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# ipv6 mld query-interval 50
```

ipv6 mld robustness

Configures the number of times that the device sends each multicast listening discovery (MLD) message from an interface.

Syntax

ipv6 mld robustness *num*

no ipv6 mld robustness *num*

Command Default

The MLD robustness is 2 seconds.

Parameters

num

Number in seconds, from 2 through 7. The default is 2.

Modes

Global configuration mode.

VRF configuration mode.

Usage Guidelines

The **no** form of this command resets the query interval to the default of 2 seconds.

Configure a higher value to ensure high MLD reliability.

Examples

This example configures the MLD robustness to 3 seconds.

```
Device(config)# ipv6 mld robustness 3
```

This example configures the MLD robustness for a VRF to 3 seconds.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# ipv6 mld robustness 3
```

ipv6 mld static-group

Configures one or more physical ports to be a permanent (static) member of a multicast listening discovery (MLD) group based on the range or count.

Syntax

ipv6 mld static-group *multicast-group-addr* [**count** *count-number* | **to** *multicast-group-addr*] [**ethernet** *stackid/slot/portnum*] [**ethernet** *stackid/slot/portnum* **to ethernet** *stackid/slot/portnum*]]

no ipv6 mld static-group *multicast-group-addr* [**count** *count-number* | **to** *multicast-group-addr*] [**ethernet** *stackid/slot/portnum*] [**ethernet** *stackid/slot/portnum* **to ethernet** *stackid/slot/portnum*]]

Command Default

The port is not added to MLD group.

Parameters

ip-addr

The address of the static MLD group.

count *count-number*

Specifies the number of static MLD groups The range is 2 through 256.

to

Specifies a range of addresses.

ethernet *stackid/slot/portnum*

Specifies the ID of the physical port that will be a member of the MLD group. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id. You can configure a single port or a list of ports, separated by a space.

Modes

Interface configuration mode.

Usage Guidelines

The **no** form of this command removes the port or ports from the MLD group.

You can specify as many port numbers as you want to include in the static group.

For a virtual routing interface (ve), specify the physical Ethernet ports on which to add the group address.

Examples

The following example configures two static groups, starting from ff0d::1, without having to receive an MLDv1 report on a virtual Ethernet interface,

```
device# configure terminal
device(config)# interface ethernet 10000 1/1/2
device(config-if-e10000-1/1/2)# ipv6 mld static-group ff0d::1 count 2
```

The following example configures two static MLD groups, starting from ff0d::1, using the **to** keyword.

```
device# configure terminal
device(config)# interface ethernet 10000 1/1/2
device(config-if-e10000-1/1/2)# ipv6 mld static-group ff0d::1 to ff0d::2
```

The following example configures two static MLD groups on virtual ports starting from ff0d::1 using the **count** keyword.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld static-group ff0d::1 count 2 ethernet 1/5/2
```

The following example configures two static groups on virtual ports starting from ff0d::1 using the **to** keyword.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld static-group ff0d::1 to ff0d::2 ethernet 1/5/2
```

ipv6 mld tracking

Enables multicast listening discovery (MLD) tracking on a virtual interface.

Syntax

ipv6 mld tracking

no ipv6 mld tracking

Command Default

Multicast tracking is disabled on the virtual interface.

Modes

Virtual interface configuration mode

Usage Guidelines

The **no** form of this command restores the default; tracking is disabled.

When MLD tracking is enabled, a Layer 3 device tracks all clients that send membership reports. When a Leave message is received from the last client, the device immediately stops forwarding to the physical port, without waiting 3 seconds to confirm that no other clients still want the traffic.

Examples

This example enables multicast tracking on a virtual interface.

```
device# configure terminal
device(config)# interface ve 13
device(config-vif-13)# ipv6 mld tracking
```

ipv6 mroute

Configures a static IPv6 route to direct multicast traffic along a specific path.

Syntax

ipv6 mroute [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length* { **ethernet** *stackid* / *slot* / *portnum* | **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

no ipv6 mroute [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length* { **ethernet** *stackid* / *slot* / *portnum* | **ve** *num* | **tunnel** *num* } [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default

No static IPv6 multicast route is configured.

Parameters

vrf *vrf-name*
Configures a static mroute for this virtual routing and forwarding (VRF) route.

ipv6-address-prefix/prefix-length
Configures the destination IPv6 address and prefix for which the route should be added.

ethernet *stackid* / *slot* /*portnum*
Configures an Ethernet interface as the route path.

ve *num*
Configures a virtual interface as the route path.

tunnel *num*
Configures a tunnel interface as the route path.

cost
Configures a metric for comparing the route to other static routes in the IPv6 static route table that have the same destination. The range is 1 to 16; the default is 1.

distance *distance-value*
Configures the route's administrative distance. The range is 1 to 255; the default is 1.

name *name*
Name for this static route.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command deletes a previously configured static multicast route.

Connected routes on PIM enabled interfaces are automatically added to the mRTM table.

Examples

The following example configures a static IPv6 mroute to directly connected network 2020::0/120 on virtual interface ve 130.

```
Device(config-vrf)# ipv6 mroute 2020::0/120 ve 130
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mroute (next hop)

Configures a static IPv6 multicast route (mroute) with a next hop.

Syntax

ipv6 mroute [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

no ipv6 mroute [**vrf** *vrf-name*] *ipv6-address-prefix/prefix-length next-hop address* [*cost*] [**distance** *distance-value*] [**name** *name*]

Command Default

No next-hop static IPv6 multicast route is configured.

Parameters

vrf *vrf-name*
Configures a static mroute for this virtual routing and forwarding (VRF) route.

ipv6-address-prefix/prefix-length
Configures the destination IPv6 address and prefix for which the route should be added.

next-hop address
Configures a next-hop address as the route path.

cost
Configures a metric for comparing the route to other static routes in the static route table that have the same destination. The range is 1-16; the default is 1.

distance *distance-value*
Configures the route's administrative distance. The range is 1 to 255; the default is 1.

name *name*
Name for this static route.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command deletes a previously configured next-hop static IPv6 multicast route.

Examples

The following example configures a next-hop static multicast IPv6 route to network 2020::0/120 with 2022::0/120 as the next hop.

```
Device(config-vrf)# ipv6 mroute 2020::0/120 2022::0/120
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mroute next-hop-enable-default

Enables the option to use the default multicast route (mroute) to resolve a static IPv6 mroute next hop.

Syntax

ipv6 mroute [**vrf** *vrf-name*] **next-hop-enable-default**

no ipv6 mroute [**vrf** *vrf-name*] **next-hop-enable-default**

Command Default

Static mroutes are not resolved using the default mroute.

Parameters

vrf *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of this command disables the default IPv6 mroute option for next hops.

Examples

The following example enables the use of the default mroute to resolve a static IPv6 mroute next hop:

```
Device(config-vrf)# ipv6 mroute next-hop-enable-default
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 mroute next-hop-recursion

Configures the recursion level when using static mroutes to resolve a static mroute next hop.

Syntax

ipv6 mroute [**vrf** *vrf-name*] **next-hop-recursion** *num*

no ipv6 mroute [**vrf** *vrf-name*] **next-hop-recursion**

Command Default

The recursion level for resolving a static mroute next hop is 3.

Parameters

vrf *vrf-name*

Configures a static mroute for this virtual routing and forwarding (VRF) route.

num

Specifies the recursion level used to resolve a static mroute next hop. The range of possible values is from 1 to 10. This is not used in the **no** form.

Modes

VRF configuration mode

Usage Guidelines

The **no** form restores the default recursion level for resolving a static mroute next hop, which is 3. You do not specify a value for the recursion level.

Examples

The following example configures the recursion level for resolving a static mroute next hop to 7:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ipv6 mroute next-hop-recursion 7
```

The following example configures the recursion level for resolving a static mroute next hop to 2:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# ipv6 mroute next-hop-recursion 2
```

The following example restores the default recursion level of 3 for resolving a static mroute next hop:

```
device(config)# vrf vrf2
device(config-vrf-vrf2)# no ipv6 mroute next-hop-recursion
```

History

Release version	Command history
8.0.10a	This command was introduced.

ipv6 multicast age-interval

Configures the time that group entries can remain in a multicast listening discovery (MLD) group table.

Syntax

ipv6 multicast age-interval *interval*

no ipv6 multicast age-interval *interval*

Command Default

Group entries can remain in the MLD group table for up to 260 seconds.

Parameters

interval

Specifies the time, in seconds, that group entries can remain in the MLD group table. The range is 20 through 7200 seconds. The default is 260 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default age interval to 260 seconds.

When a device receives a group membership report it makes an entry for that group in the MLD group table. You can configure the **ipv6 multicast age-interval** to specify how long the entry can remain in the table before the device receives another group membership report. When multiple devices are connected, they must all be configured for the same age interval, which must be at least twice the length of the query interval, so that missing one report does not stop traffic.

Non-querier age intervals must be the same as the age interval of the querier.

Examples

This example configures the MLD group-table age interval to 280 seconds.

```
Device(config)#ipv6 multicast age-interval 280
```

ipv6 multicast disable-flooding

Disables the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

Syntax

ipv6 multicast disable-flooding

no ipv6 multicast disable-flooding

Command Default

The device floods unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

Modes

Global configuration mode

Usage Guidelines

NOTE
Disabling the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN is supported only on the following platforms:

- ICX 6650
- ICX 7750 (standalone and stacking)

The **no** form of this command enables the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

In releases prior to FastIron 8.0.30, support for this command on the Brocade ICX 7750 was for devices in standalone mode only.

After the hardware forwarding database (FDB) entry is made, the multicast traffic is switched only to the VLAN hosts that are members of the multicast group. This can avoid congestion and loss of traffic on the ports that have not subscribed to this IPv6 multicast traffic.

Examples

The following example disables flooding of unregistered IPv6 multicast frames.

```
Device(config)# ipv6 multicast disable-flooding
```

History

Release version	Command history
08.0.01	This command was introduced.

ipv6 multicast leave-wait-time

Configures the wait time before stopping traffic to a port when a leave message is received.

Syntax

ipv6 multicast leave-wait-time *num*

no ipv6 multicast leave-wait-time *num*

Command Default

The wait time is 2 seconds.

Parameters

num

Specifies the time, in seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 1 through 5 seconds. The default is 2 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default wait time.

The device sends group-specific queries once per second to ask if any client in the same port still needs the group. Because of internal timer granularity, the actual wait time is between n and (n+1) seconds (n is the configured value).

Examples

This example configures the maximum time a client can wait before responding to a query as 1 second.

```
Device(config)#ipv6 multicast leave-wait-time 1
```

ipv6 multicast mcache-age

Configures the time for an mcache to age out when it does not receive traffic.

Syntax

ipv6 multicast mcache-age *num*

no ipv6 multicast mcache-age *num*

Command Default

The mcache ages out after the default age-out interval, which is 180 seconds for FSX 800/1600, ICX 7750, ICX 7450, and ICX 7250 devices, and 60 seconds for all other devices.

Parameters

num

Specifies the time, in seconds, the device should wait before stopping traffic to a port when a leave message is received The range is 60 through 3600 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default mcache age-out time.

You can set the time for a multicast cache (mcache) to age out when it does not receive traffic. Two seconds before an mcache is aged out, the device mirrors a packet of the mcache to the CPU to reset the age. If no data traffic arrives within two seconds, the mcache is deleted.

NOTE
On devices that support MAC-based MLD snooping (like the FSX, ICX 7750, ICX7450, and ICX 7250), more than one mcache can be mapped to the same destination MAC. When an mcache entry is deleted, the MAC entry may not be deleted. If you configure a lower value, the resource consumed by idle streams is quickly removed, but packets are mirrored to the CPU more frequently. Configure a higher value only when data streams are arriving consistently.

Examples

This example configures the time for an mcache to age out to 180 seconds.

```
Device(config)#ipv6 multicast mcache-age 180
```

ipv6 multicast query-interval

Configures how often the device sends group membership queries when the multicast listening discovery (MLD) mode is set to active.

Syntax

ipv6 multicast query-interval *interval*

no ipv6 multicast query-interval *interval*

Command Default

Queries are sent every 125 seconds.

Parameters

interval

Specifies the time, in seconds, between queries. The range is 10 through 3600 seconds. The default is 125 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the query interval to 125 seconds.

If the MLD mode is set to active, you can modify the query interval, which specifies how often the Brocade device sends group membership queries. When multiple queriers connect together, all queriers should be configured with the same interval.

Examples

The following example configures the query interval to 120 seconds.

```
device#configure terminal
device(config)#ipv6 multicast query-interval 120
```

ipv6 multicast report-control

Limits report forwarding within the same group to no more than once every 10 seconds.

Syntax

ipv6 multicast report-control

no ipv6 multicast report-control

Command Default

A device in passive mode forwards reports and leave messages from clients to the upstream router ports that are receiving queries.

Modes

Global configuration mode

Usage Guidelines

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

> **NOTE**
> This feature applies only to multicast listening discovery (MLD) version 1. The leave messages are not rate limited.

This rate-limiting does not apply to the first report answering a group-specific query.

Configure this command to alleviate report storms from many clients answering the upstream router query.

Examples

This example limits the rate that reports are forwarded.

```
Device(config)#ipv6 multicast-report-control
```

ipv6 multicast verbose-off

Turns off error or warning messages that are displayed when the device runs out of software resources or when it receives packets with the wrong checksum or groups.

Syntax

ipv6 multicast verbose-off

no ipv6 multicast verbose-off

Command Default

Messages are displayed.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default display of messages.

Examples

This example turns off the display of messages.

```
device# configure terminal
device(config)# ipv6 multicast verbose-off
```

ipv6 multicast version

Configures the multicast listening discovery (MLD) version for snooping globally.

Syntax

ipv6 multicast version [**1** | **2**]

no ipv6 multicast version

Command Default

MLD version 1 is configured.

Parameters

1

Configures MLD version 1.

2

Configures MLD version 2.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the version to MLD version 1.

You can configure the MLD version for individual VLANs, or individual ports within VLANs. If no MLD version is specified for a VLAN, the globally configured MLD version is used. If an MLD version is specified for individual ports in a VLAN, those ports use that version instead of the version specified for the VLAN or the globally specified version. The default is MLD version 1.

Examples

This example specifies MLD version 2 on a device.

```
Device(config)#ipv6 multicast version 2
```

ipv6 multicast-boundary

Defines multicast boundaries for PIM-enabled interfaces.

Syntax

ipv6 multicast-boundary *acl-spec*

no ipv6 multicast-boundary *acl-spec*

Command Default

Boundaries are not defined.

Parameters

acl-spec

Specifies the number or name identifying an access control list (ACL) that controls the range of group addresses affected by the boundary.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command removes the boundary on a PIM-enabled interface.

You can use standard ACL syntax to configure an access list.

Examples

This example defines a boundary named MyAccessList for a PIM-enabled interface.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e1000-1/2)#ipv6 multicast-boundary MyAccessList
```

ipv6 multicast-routing rpf-check mac-movement

Triggers Reverse Path Forwarding (RPF) check on MAC movement for directly connected sources and sends a MAC address movement notification to the Protocol Independent Multicast (PIM) module which results in PIM convergence.

Syntax

ipv6 multicast-routing rpf-check mac-movement

no ipv6 multicast-routing rpf-check mac-movement

Command Default

RPF check on MAC movement for directly connected sources is not enabled.

Modes

Global configuration mode

Usage Guidelines

PIM convergence on MAC movement is applicable only in a topology where the multicast source port and PIM routers are in the same Layer 2 domain.

IPv6 PIM Dense mode is not supported for PIM convergence on MAC movement.

The **ipv6 multicast-routing rpf-check mac-movement** command is not supported on the Brocade ICX 6650, Brocade ICX 7250, and FSX 800/FSX 1600 devices.

The **no** form of the command disables RPF check on MAC movement for directly connected sources.

Examples

The following example configures RPF check on MAC movement for directly connected sources.

```
device(config)# ipv6 multicast-routing rpf-check mac-movement
```

History

Release version	Command history
08.0.10h	This command was introduced.
08.0.30	Support for the **ipv6 multicast-routing rpf-check mac-movement** command was added in 08.0.30 and later releases.

ipv6 nd router-preference

Configures the IPv6 router advertisement preference value to low or high (medium is the default). IPv6 router advertisement preference enables IPv6 router advertisement (RA) messages to communicate default router preferences from IPv6 routers to IPv6 hosts in network topologies where the host has multiple routers on its Default Router List.

Syntax

ipv6 nd router-preference [**low** | **medium** | **high**]

no ipv6 nd router-preference [**low** | **medium** | **high**]

Command Default

The IPv6 router advertisement preference value is set to medium.

Parameters

low

The two-bit signed integer (11) indicating the preference value ''low".

medium

The two-bit signed integer (00) indicating the preference value "medium". This is the default preference value.

high

The two-bit signed integer (01) indicating the preference value "high".

Modes

Interface configuration mode

Usage Guidelines

The **no** form disables IPv6 router preference.

Examples

The following example configures IPv6 RA preference for IPv6 routers:

```
device #configure terminal
device (config)# interface ethernet 2/3
device (config-if-eth2/3)# ipv6 nd router-preference low
```

History

Release version	Command history
08.0.10	This command was introduced.

ipv6 nd skip-interface-ra

Disables the default interface-level IPv6 RA messages on an interface configured with IPv6 VRRP or VRRP-E.

Syntax

ipv6 nd skip-interface-ra

no ipv6 nd skip-interface-ra

Command Default

The IPv6-enabled interface sends the default IPv6 Router Advertisement (RA) messages. The IPv6 VRRP or VRRP-E instance configured on the interface also sends its virtual-IPv6 RA messages on the same interface. A connected IPv6 host receives these two different IPv6 RA messages with the same source address from this IPv6 router interface.

Modes

Interface configuration mode

Usage Guidelines

NOTE
This command is valid only on an interface configured with IPv6 VRRP or VRRP-E.

The **no** form of this command enables the default interface-level IPv6 RA messages on an interface configured with IPv6 VRRP or VRRP-E.

By default, all IPv6-enabled interfaces send IPv6 Router Advertisement (RA) messages. If you configure an IPv6 VRRP or VRRP-E instance on an interface, the VRRP/ VRRP-E instance also sends its IPv6 RA messages for the virtual IPv6 address on the same interface with the same source address. An IPv6 host cannot identify the valid IPv6 address for this router interface because of these two different IPv6 RA messages with the same source address from the same IPv6 router interface. To avoid this, run this command to disable the default interface-level IPv6 RA messages on an interface configured with IPv6 VRRP or VRRP-E.

Examples

The following example disables the default interface-level IPv6 RA messages on an ethernet interface 1/1/7 configured with IPv6 VRRP or VRRP-E.

```
device(config)# interface ethernet 1/1/7
device(config-if-e1000-1/1/7)# ipv6 address 2002:AB3::2/64
device(config-if-e1000-1/1/7)# ipv6 nd  skip-interface-ra
```

History

Release version	Command history
08.0.01	This command was introduced.

ipv6 neighbor inspection

Configures the static neighbor discovery (ND) inspection entries.

Syntax

ipv6 neighbor inspection *ipv6-address mac-address*

no ipv6 neighbor inspection *ipv6-address mac-address*

Command Default

Static ND inspection entries are not configured.

Parameters

ipv6-address
Configures the IPv6 address of the host.

mac-address
Configures the MAC address of the host.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Use the **ipv6 neighbor inspection** command to manually configure static ND inspection entries for hosts on untrusted ports. During ND inspection, the IPv6 address and MAC address entries in the ND inspection table are used to validate the packets received on untrusted ports.

The **no** form of the command disables static ND inspection entries.

Examples

The following example displays the configuration of a static ND inspection entry.

```
device(config)# ipv6 neighbor inspection 2001::1 0000.1234.5678
```

The following example displays the configuration of a static ND inspection entry for VRF 3.

```
device(config)# vrf 3
device(config-vrf-3)# ipv6 neighbor inspection 2001::100 0000.0000.4567
```

History

Release version	Command history
08.0.20	This command was introduced.

ipv6 neighbor inspection vlan

Configures and enables neighbor discovery (ND) inspection on a VLAN to inspect the IPv6 packets from untrusted ports.

Syntax

ipv6 neighbor inspection vlan *vlan-number*

no ipv6 neighbor inspection vlan *vlan-number*

Command Default

IPv6 neighbor inspection is not enabled.

Parameters

vlan-number

Configures the ID of the VLAN.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

When you configure this command, IPv6 packets from untrusted ports on the VLAN undergo ND inspection.

The **no** form of the command disables ND inspection.

Examples

The following example enables ND inspection on VLAN 10.

```
device(config)# ipv6 neighbor inspection vlan 10
```

The following example enables ND inspection on VLAN 10 of VRF 3.

```
device(config)# vrf 3
device(config-vrf-3)# ipv6 neighbor inspection vlan 10
```

History

Release version	Command history
08.0.20	This command was introduced.

ipv6 pim border

Configures an interface to be on a PIM Sparse domain border.

Syntax

ipv6 pim border

no ipv6 pim border

Command Default

The interface is not configured as a border device.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command removes the boundary on a PIM-enabled interface.

You must enable PIM globally before you enable it on an interface.

Examples

This example configures Ethernet interface 3/2/4 to be on a PIM Sparse domain border.

```
device(config) interface ethernet 3/2/4
Device(config-if-e10000-3/2/4)# ipv6 pim border
```

ipv6 pim dr-priority

Configures the designated router (DR) priority on IPv6 interfaces.

Syntax

ipv6 pim dr-priority *priority-value*

no ipv6 pim *priority-value*

Command Default

The DR priority value is 1.

Parameters

priority-value

Specifies the DR priority value as an integer. The range is 0 through 65535. The default is 1.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the default DR priority value, 1.

You must enable PIM globally before you enable it on an interface.

If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IPv6 address on that subnet is elected as the DR.

The DR priority information is used in the DR election only if all the PIM devices connected to the subnet support the DR priority option. If at least one PIM device on the subnet does not support this option, the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IPv6 address on the subnet is declared the DR regardless of the DR priority values.

Examples

This example configures a DR priority value of 50 on Ethernet interface 3/2/4.

```
device(config) interface ethernet 3/2/4
Device(config-if-e10000-3/2/4)# ipv6 pim dr-priority 50
```

This example configures a DR priority value of 50 on a virtual Ethernet interface.

```
Device(config)# interface ve 10
Device(config-vif-10)# ipv6 pim dr-priority 50
```

ipv6 pim neighbor-filter

Determines which devices can become PIM neighbors.

Syntax

ipv6 pim neighbor-filter *acl-name*

no ipv6 pim *acl-name*

Command Default

Neighbor filtering is not applied on the interface.

Parameters

acl-name

Specifies the access-control list (ACL)that identifies the devices you want to permit and deny participation in PIM.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command removes any neighbor filtering applied on the interface.

You must enable PIM globally before you enable it on an interface.

You can configure the **ipv6 pim neighbor-filter** command in either Dense mode (DM) or Sparse mode (SM).

Configure the **access-list** command to create an ACL defining the devices you want to permit and deny participation in PIM.

Examples

This example prevents the host from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ipv6 pim neighbor-filter
```

This example configures an ACL named 10 to deny a host and then prevents that host, 1001::1/96, identified in that ACL from becoming a PIM neighbor on interface Ethernet 1/3/24.

```
Device(config)# access-list 10  deny host 1001::1/96
Device(config)# access-list 10 permit any
Device(config)# interface ethernet 1/3/24
Device(config-if-e10000-1/3/24)# ipv6 pim neighbor-filter 10
```

History

Release version	Command history
8.0.20a	This command was introduced.

ipv6 pim-sparse

Enables PIM Sparse on an IPv6 interface.

Syntax

ipv6 pim-sparse

no ipv6 pim-sparse

Command Default

PIM Sparse is not enabled on the IPv6 interface.

Modes

Interface configuration mode

Usage Guidelines

The **no ipv6 pim-sparse** command removes the PIM sparse configuration from the IPv6 interface.

Examples

This example adds an IPv6 interface to port 1/2/2, then enables PIM Sparse on the interface.

```
Device(config)# interface ethernet 1/2/2
Device(config-if-e10000-2/2)# ipv6 address a000:1111::1/64
Device(config-if-e10000-2/2)# ipv6 pim-sparse
```

ipv6-proto

Configures an IPv6 protocol-based VLAN.

Syntax

ipv6-proto [**name** *string*]

no ipv6-proto [**name** *string*]

Command Default

An IPv6 protocol-based VLAN is not configured.

Parameters

name *string*

Specifies the IPv6 protocol-based VLAN name. The maximum length of the string is 32 characters.

Modes

VLAN configuration mode

Usage Guidelines

You can configure a protocol-based VLAN as a broadcast domain for IPv6 traffic. When the Layer 3 switch receives an IPv6 multicast packet (a packet with 06 in the version field and 0xFF as the beginning of the destination address), the Layer 3 switch forwards the packet to all other ports.

The **no** form of the command disables the IPv6 protocol VLAN.

Examples

The following example configures the IPv6 protocol-based VLAN.

```
device(config)# vlan 2
device(config-vlan-2)# ipv6-proto name V6
```

ipv6 raguard policy

Configures the specified Router Advertisement (RA) guard policy and enters RA guard policy configuration mode.

Syntax

ipv6 raguard policy *name*

no ipv6 raguard policy *name*

Parameters

name

An ASCII string indicating the name of the RA guard policy to configure.

Modes

Global configuration mode

RA guard policy configuration mode

Usage Guidelines

You can configure up to 256 RA guard policies.

The **no** form of this command deletes the specified RA guard policy.

Examples

The following example configures an RA guard policy and enters RA guard policy configuration mode:

```
Brocade(config)# ipv6 raguard policy policy1
Brocade(ipv6-RAG-policy policy1)#
```

ipv6 raguard vlan

Associates a Router Advertisement (RA) guard policy with a VLAN.

Syntax

ipv6 raguard vlan *vlan-number* **policy** *name*

no ipv6 raguard vlan *vlan-number* **policy** *name*

Parameters

vlan-number

Configures the ID number of the VLAN to which the specified RA guard policy should be associated. Valid range is from 1 to 4095.

policy

Associates a RA guard policy to the VLAN.

name

Specifies the name of the RA guard policy to be associated with the VLAN.

Modes

Global configuration mode

Usage Guidelines

A VLAN can have only one association with a RA guard policy. If you try to associate a new RA guard policy with a VLAN that is already associated with a policy, the new RA guard policy replaces the old one.

no

Examples

The following example associates RA guard policy named p1 with VLAN 1:

```
Brocade(config)# ipv6 raguard vlan 1 policy p1
```

ipv6 raguard whitelist

Configures the Router Advertisement (RA) guard whitelist and adds the IPv6 address as the allowed source IP address.

Syntax

ipv6 raguard whitelist *whitelist-number* **permit** *ipv6-address*

no ipv6 raguard whitelist *whitelist-number* **permit** *ipv6-address*

Parameters

whitelist-number
Configures the unique identifier for the RA guard whitelist. Valid values are 0 to 255.

permit
Configures the specified IPv6 address as the allowed source IP address to the RA guard whitelist.

ipv6-address
Configures the source IPv6 address. The address should be in the format X:X::X:X or X:X::X:X/M.

Modes

Global configuration mode

Usage Guidelines

You can configure source IP addresses from which RAs are permitted.

You can configure up to 64 RA guard whitelists, and each whitelist can have a maximum of 128 entries.

To remove the RA guard whitelist, use the **no** form the command without the **permit** keyword.

To remove a particular IPv6 address from the whitelist, use the **no** form of the command with the **permit***ipv6-address* keyword-variable pair.

When a whitelist associated with an RA guard policy is removed, all the entries in the whitelist are also removed. All the RAs are dropped because there is no whitelist associated with the RA guard policy.

Examples

The following example configures an RA guard whitelist with the allowed source IP address:

```
Brocade(config)# ipv6 raguard whitelist 1 permit fe80:db8::db8:10
```

The following example removes an RA guard whitelist:

```
Brocade(config)# no ipv6 raguard whitelist 1
```

The following example removes a particular IPv6 address from the RA guard whitelist:

```
Brocade(config)# no ipv6 raguard whitelist 1 permit fe80:db8::db8:10
```

ipv6 route

Configures a static route.

Syntax

ipv6 route [**vrf** *vrf-name*] *dest-ipv6-prefix* [**ethernet** *stackid/slot/port* | **ve** *ve-num*] *next-hop-ipv6-address* [*metric*] [**distance** *number*]

no ipv6 route [**vrf** *vrf-name*] *dest-ipv6-prefix* [**ethernet** *stackid/slot/port* | **ve** *ve-num*] *next-hop-ipv6-address* [*metric*] [**distance** *number*]

ipv6 route [**vrf** *vrf-name*] *dest-ipv6-prefix* { **tunnel** *num* | **null0** } [*metric*] [**distance** *number*]

no ipv6 route [**vrf** *vrf-name*] *dest-ipv6-prefix* { **tunnel** *num* | **null0** } [*metric*] [**distance** *number*]

ipv6 route [**vrf** *vrf-name*] *dest-ipv6-prefix* { **next-hop ospf** | **next-hop-enable-default** | **next-hop-recursion** [*number*] }

no ipv6 route [**vrf** *vrf-name*] *dest-ipv6-prefix* { **next-hop ospf** | **next-hop-enable-default** | **next-hop-recursion** [*number*] }

Command Default

By default, static routes take precedence over routes learned by routing protocols.

Parameters

vrf *vrf-name*
Specifies the VRF that contains the next-hop router (gateway) for the route.

dest-ipv6-prefix
Specifies the destination IPv6 address.

ethernet *stackid/slot/port*
Configures the outgoing interface as the specified Etherent interface.

ve *ve-num*
Configures the outgoing interface as the specified Virtual Etherent interface.

next-hop-ipv6-address
Specifies the IPv6 address of a next-hop gateway.

metric
Specifies the route's metric. The value can range from 1 to 16. The default value is 1.

distance *number*
Specifies the route's administrative distance. The default value is 1.

tunnel *num*
Configures the outgoing interface as the specified tunnel interface.

null0
Configures to drop packets with this destination.

next-hop ospf
Configures OSPF routes to be used for nexthop resolution of the static route IPv6 nexthop.

next-hop-enable-default
Configures to use the default route to resolve static route nexthop.

next-hop-recursion
Configures to use the static route to resolve static route nexthop.

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 removes the static IPv6 route configuration from a VRF.

Examples

The following example shows how to configure a static IPv6 route for a destination network with the prefix 2001:DB8::0/32, a next-hop gateway with the global address 2001:DB8:0:ee44::1, in the non-default VRF named "blue".

```
device(config)# ipv6 route vrf blue 2001:DB8::0/32 2001:DB8:0:ee44::1
```

ipv6 router pim

Enables IPv6 PIM-Sparse mode for IPv6 routing globally or on a specified VRF.

Syntax

ipv6 router pim [**vrf** *vrf-name*]

no ipv6 router pim [**vrf** *vrf-name*]

Command Default

IPv6 PIM-Sparse mode is not enabled.

Parameters

vrf *vrf-name*
Specifies a VRF instance.

Modes

Global configuration mode.

VRF configuration mode.

Usage Guidelines

The **no** form of this command removes the IPv6 PIM-Sparse mode configuration.

Examples

The following example enables IPv6 PIM-Sparse mode on a VRF named blue.

```
Device(config)# ipv6 router pim vrf blue
```

ipv6 traffic-filter

Applies an 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

The ACL is not applied to an interface.

Parameters

acl-name

Applies the specified ACL to the interface traffic.

in

Applies the specified IPv6 ACL to incoming IPv6 packets on the interface.

out

Applies the specified IPv6 ACL to outgoing IPv6 packets on the interface.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command removes the association of the ACL with interface traffic.

NOTE
The command is not supported on FSX devices.

Examples

The following example applies the ACL "acl1" to the interface 1/1/1 .

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# ipv6 traffic-filter acl1 in
```

ipv6-address auto-gen-link-local

Generates a virtual link-local IPv6 address and assigns it as the virtual IPv6 address for a VRRPv3 instance.

Syntax

ipv6-address auto-gen-link-local

no ipv6-address auto-gen-link-local

Modes

VRRP sub-configuration mode

Usage Guidelines

The **no** form of this command deletes the auto-generated virtual link-local IPv6 address for the VRRP v3 instance.

The default VRRPv3 implementation allows only the link-local address that is configured on a physical interface to be used as the virtual IPv6 address of a VRRPv3 instance. This limits configuring a link-local address for each VRRP instance on the same physical interface because there can be only one link-local address per physical interface. You can use this command on the owner or backup router to generate a virtual link-local IPv6 address from the virtual MAC address of a VRRPv3 instance and assign it as the virtual IPv6 address for the VRRPv3 instance. This auto-generated link-local IPv6 address is not linked to any physical interface on the router.

Examples

The following example generates a virtual link-local IPv6 address and its allocation as the virtual IPv6 address of a VRRPv3 cluster on an owner router.

```
device(config)# interface ve 3
device(config-vif-3)# ipv6 vrrp vrid 2
device(config-vif-3-vrid-2)# owner
device(config-vif-3-vrid-2)# ipv6-address auto-gen-link-local
device(config-vif-3-vrid-2)# activate
```

History

Release version	Command history
08.0.01	This command was introduced.

ipv6-neighbor inspection trust

Enables trust mode for specific ports.

Syntax

ipv6-neighbor inspection trust [**vrf** *vrf-name*]

no ipv6-neighbor inspection trust [**vrf** *vrf-name*]

Command Default

Trust mode is not enabled. When you enable ND inspection on a VLAN, by default, all the interfaces and member ports are considered as untrusted.

Parameters

vrf
: Specifies the VRF instance.

vrf-name
: Specifies the ID of the VRF instance.

Modes

Interface configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command disables trust mode on ports.

Examples

The following example displays the trust mode configuration for ports.

```
device(config)# interface ethernet 1/1/3
device(config-if-e1000-1/1/3)# ipv6-neighbor inspection trust
```

The following example displays the trust mode configuration on a port on VRF 3.

```
device(config-if-e1000-1/1/1)# ipv6-neighbor inspection trust vrf 3
```

History

Release version	Command history
08.0.20	This command was introduced.

ipv6 unicast-routing

Enables the forwarding of IPv6 traffic on a Layer 3 swtich.

Syntax

ipv6 unicast-routing

no ipv6 unicast-routing

Command Default

The forwarding of IPv6 traffic is not enabled.

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 unicast routing.

Examples

The following example enables IPv6 unicast routing.

```
device(config)# ipv6 unicast-routing
```

ipx-network

Configures the IPX network protocol-based VLANs.

Syntax

ipx-network *network-number ipx-frame-type* [**name** *string*]

no ipx-network *network-number ipx-frame-type* [**name** *string*]

Command Default

An IPX network protocol-based VLAN is not configured.

Parameters

network-number

Specifies the network number in hexadecimal format.

ipx-frame-type

Defines the IPX frame encapsulation standard types. The following are the supported encapsulation standard types:

ethernet_802.2

Specifies the Ethernet 802.2 standard that can be configured for the protocol.

ethernet_802.3

Specifies the Ethernet 803.3 standard that can be configured for the protocol.

ethernet_ii

Specifies the Ethernet II standard that can be configured for the protocol.

ethernet_snap

Specifies the Ethernet subnetwork access protocol standard that can be configured for the protocol.

name *string*

Specifies the Ethernet standard name. The string can be up to 32 characters in length.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command disables the IPX network protocol-based VLAN.

Examples

The following example shows how to configure the IPX network protocol-based VLAN.

```
device(config)# vlan 20 name IPX_VLAN by port
device(config-vlan-10)# untagged ethernet 1/2/1 to 1/2/6
added untagged port ethe 1/2/1 to 1/2/6 to port-vlan 20.
device(config-vlan-10)# ipx-network abcd ethernet_ii name Eng-LAN
```

ipx-proto

Configures the IPX protocol-based VLANs.

Syntax

ipx-proto [**name** *string*]

no ipx-proto [**name** *string*]

Command Default

An IPX protocol-based VLAN is not configured.

Parameters

name *string*

The IPX protocol-based VLAN name. The name can be up to 32 characters in length.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command removes the IPX protocol-based VLAN.

Examples

The following example shows the how to configure an IPX protocol-based VLAN.

```
device(config)# vlan 10 by port
device(config-vlan-10)# untagged ethernet 1/1/1 to 1/1/6
added untagged port ethe 1/1/1 to 1/1/6 to port-vlan 30.
device(config-vlan-10)# ip-proto name IP_Prot_VLAN
```

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.

When JITC is enabled, the MD5 authentication scheme for NTP is disabled.

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.

Examples

The following example enables the JITC mode.

```
device(config)# jitc enable
```

History

Release version	Command history
08.0.20a	This command was introduced.

jitc show

Displays the status of the JITC mode.

Syntax

jitc show

Modes

Global configuration mode

Privileged EXEC mode

Command Output

The **jitc show** command displays the following information.

Output field	Description
JITC mode	Displays the status of the JITC mode.
SSH AES-CTR mode	Displays the status of the SSH AES-CTR mode.
SSH AES-CBC mode	Displays the status of the SSH AES-CBC mode.

Examples

The following example shows the output of the **jitc show** command.

```
device(config)#jitc show
JITC mode : Enabled
Management Protocol Specific:
SSH AES-CTR mode : Enabled
SSH AES-CBC mode : Disabled
```

History

Release version	Command history
08.0.20a	This command was introduced.

join-timer leave-timer leaveall-timer

Changes the Join, Leave, and Leaveall timers for GVRP counters.

Syntax

join-timer *join-timer-ms* **leave-timer** *leave-timer-ms* **leaveall-timer** *leaveall-timer-ms*

Command Default

The default value for the Join timer is 200 ms. The default value for the Leave timer is 600 ms. The default value for the Leaveall timer is 10,000 ms.

Parameters

join-timer-ms

Specifies the maximum number of milliseconds (ms) a GVRP interface wait before sending VLAN advertisements on the interfaces. You can set the Join timer to a value from 200 to one third the value of the Leave timer.

leave-timer-ms

Specifies the number of milliseconds a GVRP interface waits after receiving a Leave message on the port to remove the port from the VLAN indicated in the Leave message. You can set the Leave timer to a value from three times the Join timer value to one fifth the value of the Leaveall timer.

leaveall-timer-ms

Specifies the minimum interval at which GVRP sends Leaveall messages on all GVRP interfaces. You can set the Leaveall timer to a value from five times the Leave timer value to the maximum value allowed by the software (configurable from 300,00 to 1,000,000 ms).

Modes

GVRP configuration mode

Usage Guidelines

All timer values must be in multiples of 100 ms.

The Leave timer value must be greater than or equal to three times the Join timer value. The Leaveall timer value must be greater than or equal to five times the Leave timer value.

The GVRP timers must be set to the same values on all the devices that are exchanging information using GVRP.

NOTE
When you enter this command, all the running GVRP timers are canceled and restarted using the new times specified by the command.

Examples

The following example shows how to set the Join, Leave, and Leaveall timers.

```
device(config)# gvrp-enable
device(config-gvrp)# join-timer 1000 leave-timer 3000 leaveall-timer 15000
```

jumbo

Provides jumbo frame support.

Syntax

jumbo

no jumbo

Command Default

Jumbo frame support is disabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables jumbo frame support.

Examples

The following example shows how to provide jumbo frame support.

```
device(config)# jumbo
```

Commands K - S

keep-alive-vlan

Configures a keep-alive VLAN for the cluster.

Syntax

keep-alive-vlan *vlan-ID*

no keep-alive-vlan *vlan-ID*

Command Default

A keep-alive VLAN is not configured.

Parameters

vlan-ID

Specifies the VLAN number. The values can be from 1 through 4089.

Modes

Cluster configuration mode

Usage Guidelines

Only one VLAN can be configured as a keep-alive VLAN. The keep-alive VLAN cannot be a member VLAN of the Multi-Chassis Trunking (MCT) and this VLAN can be tagged or untagged.

When the CCP is down, the following results occur:

- If the keep-alive VLAN is configured, CCRR messages are sent every second over that VLAN.
- If no packets are received from the peer device for a period of three seconds, the peer is considered down.
- If a keep-alive VLAN is not configured and both the peer devices are up, both peers continue forwarding traffic independently, when the CCP is down.

  NOTE
  Keep-alive VLAN configuration is not allowed when the client isolation mode is strict; and when the keep-alive VLAN is configured, client isolation mode cannot be configured as strict.

The **no** form of the command removes the keep-alive VLAN configuration.

Examples

The following example shows how to configure the keep-alive VLAN.

```
device(config)# cluster SX 400
device(config-cluster-SX)# keep-alive-vlan 10
```

key-server-priority

Configures the MACsec key-server priority for the MACsec Key Agreement (MKA) group.

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.

Modes

dot1x-mka-cfg-group mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

The **no** form of the command removes the previous priority setting.

During key-server election, the server with the highest priority (the server with the lowest key-server priority value) becomes the key-server.

Examples

The following example sets the key-server priority for MKA group test1 to 5.

```
device(config)#dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# key-server-priority 5
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20a	This command was modified. The key-server priority value range was increased from 0 through 127 to 0 through 255.

kill

Terminates active CLI sessions.

Syntax

kill console { **all** | *unit-number* }

kill { **ssh** | **telnet** } *session-number*

Parameters

console
Logs out console sessions in a stack.

all
Logs out all console ports on stack units that are not the Active Controller.

unit-number
Logs out the console port on a specified unit.

ssh
Terminates an active SSH session.

telnet
Terminates an active Telnet session.

session-number
The Telnet or SSH session number.

Modes

Privileged EXEC mode

Usage Guidelines

Once the AAA console is enabled, you should log out any open console ports on your traditional stack using the **kill console** command.

Examples

The following example shows how to log out from all console ports on stack units that are not the Active Controller.

```
device# kill console all
```

The following example shows how to terminate an active SSH connection.

```
device# kill ssh 1
```

lacp-timeout

Configures the timeout mode for the port.

Syntax

lacp-timeout { **long** | **short** }

no lacp-timeout { **long** | **short** }

Command Default

Begins with the short timeout period. Moves to the long timeout period after the LAG is established.

Parameters

long

Specifies a long timeout period for the port which is 120 seconds.

short

Specifies a short timeout period for the port which is 3 seconds.

Modes

LAG configuration mode

Usage Guidelines

After you configure a port timeout mode, the port remains in that timeout mode whether it is up or down and whether or not it is part of a LAG. All the ports in a LAG must have the same timeout mode. This requirement is checked when the LAG is enabled on the ports.

With the long timeout configuration, an LACPDU is sent every 30 seconds. If no response comes from its partner after three LACPDUs are sent, a timeout event occurs, and the LACP state machine transitions to the appropriate state based on its current state.

In the short timeout configuration, an LACPDU is sent every second. If no response comes from its partner after three LACPDUs are sent, a timeout event occurs, and the LACP state machine transitions to the appropriate state based on its current state. If you do not include **long** or **short**, the device operates based on the IEEE specification standards.

NOTE
The configuration of lacp-timeout is applicable to dynamic or keep-alive LAGs only.

The **no** form of the command resets the timeout mode to short.

Examples

The following example shows how to configure a port for a short LACP timeout.

```
device(config)# lag blue dynamic
device(config-lag-blue)# lacp-timeout short
```

lag

Creates a Link Aggregation Group (LAG).

Syntax

lag *lag-name* [**dynamic** [**id** *number*]]

no lag *lag-name* [**dynamic** [**id** *number*]]

lag *lag-name* [**static** [**id** *number*]]

no lag *lag-name* [**static** [**id** *number*]]

lag *lag-name* **keep-alive**

no lag *lag-name* **keep-alive**

Command Default

LAG is not configured.

Parameters

lag-name
: Specifies the name of the LAG as an ASCII string. The LAG name can be up to 64 characters in length.

dynamic
: Configures a dynamic LAG.

static
: Configures a static LAG.

id *number*
: Specifies a LAG ID. The value ranges from 1 through 2047.

keep-alive
: Configures a keep-alive LAG.

Modes

Global configuration mode

Usage Guidelines

The keep-alive LAG configuration can be used to configure a LAG for use in keep-alive applications similar to the UDLD.

A keep-alive LAG contains only one port while static and dynamic LAGs can have 1 to 8 or 1 to 12 ports depending on the device.

If you do not enter a LAG ID, the system automatically generates an ID. LAG IDs are unique for each LAG in the system. A LAG ID cannot be assigned to more than one LAG. If a LAG ID is already used, the CLI will reject the new LAG configuration and display an error message that suggests the next available LAG ID that can be used.

NOTE
The LAG ID parameter is for static and dynamic LAGs only. No explicit configuration of a LAG ID is allowed on keep-alive LAGs.

The **no** form of the command removes the LAG.

Examples

The following example shows how to configure a static LAG.

```
device(config)# lag blue static
device(config-lag-blue)#
```

The following example shows how to explicitly assign an ID to a LAG.

```
device(config)# lag blue static id 1
device(config-lag-blue)#
```

lease

Specifies the lease period for the DHCP address pool.

Syntax

lease *days hours minutes*

Parameters

days hours minutes

Specifies the lease duration in days, hours, and minutes.

Modes

DHCP server pool configuration mode.

Usage Guidelines

Examples

The following example specifies the lease period as one day, four hours and 32 minutes.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# lease 1 4 32
```

legacy-inline-power

Enables support for PoE legacy power-consuming devices.

Syntax

legacy-inline-power

no legacy-inline-power

Command Default

PoE devices automatically support most legacy power-consuming devices (devices not compliant with 802.3af 802.3at), as well as all 802.3af- and 802.3at-compliant devices.

Parameters

slotnum

Specifies the slot number.

Modes

Global configuration mode

Stack configuration mode

Usage Guidelines

The command does not require a software reload if it is entered prior to connecting the PDs. If the command is entered after the PDs are connected, the configuration must be saved (write memory) and the software reloaded after the change is placed into effect.

By default, the inline-power command reserves 30 watts.

When you disable legacy support, 802.3af and 802.3at-compliant devices are not affected.

The **no** form of the command disables support for PoE legacy power-consuming devices.

Examples

The following example shows how to enable support for legacy power-consuming devices on a non-stackable device.

```
device(config)# legacy-inline-power
```

link-config gig copper autoneg-control

Configures the maximum advertised speed on a port that has auto-negotiation enabled.

Syntax

link-config gig copper autoneg-control { **100m-auto** | **10m-auto** | **down-shift** } **ethernet** *stack-id/slot/port* [**to** *stack-id/slot/port* | [**ethernet** *stack-id/slot/port* **to** *stack-id/slot/port* | **ethernet** *stack-id/slot/port*] ...]

no link-config gig copper autoneg-control { **100m-auto** | **10m-auto** | **down-shift** } **ethernet** *stack-id/slot/port* [**to** *stack-id/slot/port* | [**ethernet** *stack-id/slot/port* **to** *stack-id/slot/port* | **ethernet** *stack-id/slot/port*] ...]

Command Default

The maximum port speed advertisement is not configured.

Parameters

100m-auto
Configures a port to advertise a maximum speed of 100 Mbps.

10m-auto
Configures a port to advertise a maximum speed of 10 Mbps.

down-shift
Enables Gbps copper ports on the Brocade device to establish a link at 1000 Mbps over a 4-pair wire when possible, or to down-shift to 100 Mbps if the medium is a 2-pair wire.

ethernet *stack-id/slot/port*
Specifies the Ethernet interface.

Modes

Global configuration mode

Usage Guidelines

Maximum port speed advertisement is not supported on Brocade ICX 7750.

The maximum port speed advertisement works only when auto-negotiation is enabled (CLI command **speed-duplex auto**). If auto-negotiation is off, the device rejects the maximum port speed advertisement configuration.

You can enable the maximum port speed advertisement on one or two ports at a time.

The **no** form of the command disables the maximum port speed advertisement.

Examples

The following command configures a maximum port speed advertisement of 10 Mbps on a port that has auto-negotiation enabled.

```
device(config)# link-config gig copper autoneg-control 10m-auto ethernet 1/1/1
```

History

Release version	Command history
8.0.30h	The **downshift** option was supported on all platforms.
8.0.30	This command was introduced in Brocade ICX 7250, but the **downshift** option was not supported.
8.0.20	This command was introduced in Brocade ICX 7450, but the **downshift** option was not supported.

link-error-disable

Configures port flap dampening on an interface.

Syntax

link-error-disable *toggle-threshold sampling-time-in-sec wait-time-in-sec*

no link-error-disable *toggle-threshold sampling-time-in-sec wait-time-in-sec*

Command Default

Port flap dampening is not configured.

Parameters

toggle-threshold

Specifies the number of times a port link state goes from up to down and down to up before the wait period is activated. The value ranges from 1 - 50.

sampling-time-in-sec

Specifies the amount of time during which the specified toggle threshold can occur before the wait period is activated. The default value is 0 seconds and indicates that the time is forever. The value ranges from 1 - 65535 seconds.

wait-time-in-sec

Specifies the amount of time the port remains disabled (down) before it becomes enabled. The value ranges from 0 - 65535 seconds. 0 indicates that the port will stay down until an administrative override occurs.

Modes

Interface configuration mode

Usage Guidelines

The Brocade device counts the number of times a port link state toggles from "up to down", and not from "down to up".

The sampling time or window (the time during which the specified toggle threshold can occur before the wait period is activated) is triggered when the first "up to down" transition occurs.

If the port link state toggles from up to down for a specified number of times within a specified period, the interface is physically disabled for the specified wait period. Once the wait period expires, the port link state is re-enabled. However, if the wait period is set to zero (0) seconds, the port link state will remain disabled until it is manually re-enabled.

When a flap dampening port becomes a member of a LAG, that port, as well as all other member ports of that LAG, will inherit the primary port configuration. This means that the member ports will inherit the primary port flap dampening configuration, regardless of any previous configuration.

You can configure the port flap dampening feature on the primary port of a LAG using the **link-errordisable** command. Once configured on the primary port, the feature is enabled on all ports that are members of the LAG. You cannot configure port flap dampening on port members of the LAG.

The **no** form of the command re-enables a port disabled by port flap dampening once the wait period expires.

A port disabled by port flap dampening is automatically re-enabled once the wait period expires; however, if the wait period is set to zero (0) seconds, you must re-enable the port using the **no** form of the command.

Examples

The following example shows how to configure port flap dampening on an interface.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# link-error-disable 10 3 10
```

link-fault-signal

Enables Link Fault Signaling (LFS) between 10 Gbps Ethernet devices.

Syntax

link-fault-signal

no link-fault-signal

Command Default

LFS is disabled by default on all Brocade FastIron devices except the Brocade ICX 6650.

Modes

Interface configuration mode

Usage Guidelines

When configured on a Brocade 10 Gbps Ethernet port, the port can detect and report fault conditions on transmit and receive ports. Brocade recommends enabling LFS on both ends of a link.

Enable LFS on any device prior to connecting the device to FastIron platforms. Any connecting device must have LFS currently enabled to ensure interoperability. When LFS is enabled on an interface, syslog messages are generated when the link goes up or down, or when the TX or RX fiber is removed from one or both sides of the link that has LFS enabled.

You can view the status of an LFS-enabled link using the **show interface** command.

The **no** form of the command disables the Link Fault Signaling (LFS).

Examples

The following example enables LFS.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# link-fault-signal
```

link-keepalive ethernet

Enables UDLD for tagged and untagged control packets.

Syntax

link-keepalive ethernet *stackid/slot/port* [[**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] | **vlan** *vlan-ID*]

no link-keepalive ethernet *stackid/slot/port* [[**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] | **vlan** *vlan-ID*]

Command Default

UDLD is not enabled.

Parameters

ethernet *stackid/slot/port*
: Specifies the Ethernet interface on which to enable UDLD.

to *stackid/slot/port*
: Specifies the end range of the Ethernet interface on which to enable UDLD.

vlan *vlan-ID*
: Specifies the ID of the VLAN that the UDLD control packets can contain.

Modes

Global configuration mode

Usage Guidelines

UDLD is supported only on Ethernet ports.

If you are specifying a VLAN ID, make sure that the VLAN ID is configured. A VLAN is specified when UDLD is configured. The port belongs to the configured VLAN as a tagged member. All the devices across the UDLD link are in the same VLAN. UDLD can be enabled on only one VLAN for a tagged port.

You must configure the same VLANs that will be used for UDLD on all devices across the network; otherwise, the UDLD link cannot be maintained.

Dynamic LAG is not supported with UDLD. If you want to configure a LAG that contains ports on which UDLD is enabled, you must remove the UDLD configuration from the ports. After you create the LAG, you can re-add the UDLD configuration.

The **no** form of the command disables UDLD for tagged and untagged control packets.

Examples

The following example shows how to enable UDLD for untagged ports.

```
device(config)# link-keepalive ethernet 1/1/1
```

The following example shows how to configure UDLD on multiple ports.

```
device(config)# link-keepalive ethernet 1/1/1 ethernet 1/2/2
```

The following example shows how to configure UDLD on a range of ports.

```
device(config)# link-keepalive ethernet 1/1/1 to 1/1/5
```

The following example enables ports to receive and send UDLD control packets tagged with a specific VLAN ID.

```
device(config)# link-keepalive ethernet 1/1/8 vlan 22
```

link-keepalive interval

Enables the interval time that UDLD sends health-check packets.

Syntax

link-keepalive interval *time*

no link-keepalive interval *time*

Command Default

By default, ports enabled for UDLD send a health-check packet once every 500 milliseconds (ms).

Parameters

time

Specifies the time that UDLD sends the health-check packets, in milliseconds. You can specify from 1 through 60, in 100 ms increments (1 is 100 ms, 2 is 200 ms, and so on). The default is 5 (500 ms).

Modes

Global configuration mode

Usage Guidelines

A low UDLD link-keepalive interval is not recommended because low UDLD link-keepalive intervals are more sensitive and prone to flaps.

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

Examples

The following example shows the UDLD interval configuration.

```
device(config)# link-keepalive interval 4
```

link-keepalive retries

Configures the maximum number of keep-alive attempts a port waits to receive a health-check reply packet from the port at the other end of the link.

Syntax

link-keepalive retries *number*

no link-keepalive retries *number*

Command Default

The default value is 7.

Parameters

number

Specifies the number of keep-alive retries to receive a health-check reply packet. The valid range is from 3 through 64.

Modes

Global configuration mode

Usage Guidelines

By default, a port waits one second to receive a health-check reply packet from the port at the other end of the link. If the port does not receive a reply, the port tries six more times by sending up to six more health-check packets. If the port still does not receive a reply after the maximum number of retries, the port goes down.

The **no** form of the command changes the number of retries to the default value.

Examples

The following example shows how to configure 10 retries as the maximum number of keep-alive attempts a port waits to receive a health-check reply packet.

```
device(config)# link-keepalive retries 10
```

link-oam

Enables the EFM-OAM protocol and enters EFM-OAM protocol configuration mode.

Syntax

link-oam

no link-oam

Command Default

The EFM-OAM protocol is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes all the EFM-OAM configurations.

Examples

The following example enables EFM-OAM protocol configuration mode.

```
device(config)# link-oam
device(config-link-oam)#
```

History

Release version	Command history
08.0.30	This command was introduced.

lldp advertise link-aggregation

Advertises link-aggregation information.

Syntax

lldp advertise link-aggregation ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port***to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise link-aggregation ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port***to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

Link-aggregation information is automatically advertised when LLDP is enabled on a global basis.

Parameters

ports
Advertises link aggregation information for the ports.

all
Advertises link aggregation information for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises link aggregation information for the specified Ethernet port.

to *stackid/slot/port*
Advertises link aggregation information for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The devices advertise link aggregation information about standard link aggregation (LACP) as well as static LAG configuration.

The link-aggregation time, length, value (TLV) indicates the following:

- Whether the link is capable of being aggregated
- Whether the link is currently aggregated
- The primary LAG port

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

Examples

The following example shows how to enable advertisement of link aggregation information for a specific Ethernet port.

```
device(config)# lldp advertise link-aggregation ports ethernet 1/1/1
```

lldp advertise mac-phy-config-status

Advertises MAC/PHY configuration and status information.

Syntax

lldp advertise mac-phy-config-status ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port***to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise mac-phy-config-status ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port***to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

The MAC/PHY configuration and status information are automatically advertised when LLDP is enabled on a global basis.

Parameters

ports
Advertises MAC/PHY configuration and status information for ports.

all
Advertises MAC/PHY configuration and status information for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises MAC/PHY configuration and status information for a specified Ethernet port.

ethernet *stackid/slot/port*
Advertises MAC/PHY configuration and status information for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The MAC and PHY configuration and status TLV includes the following information:

- Auto-negotiation capability and status.
- Speed and duplex mode.
- Flow control capabilities for auto-negotiation.
- Maximum port speed advertisement.
- If applicable, indicates if the above settings are the result of auto-negotiation during link initiation or of a manual set override action.

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

Examples

The following example shows how to enable advertisement of MAC/PHY configuration and status information for a specific Ethernet port.

```
device(config)# lldp advertise mac-phy-config-status ports ethernet 1/1/1
```

lldp advertise management-address

Advertises a management address.

Syntax

lldp advertise management-address { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise management-address { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

Management address advertising has two modes: default, or explicitly configured.

Parameters

ipv4 *ipv4-address*
: Specifies an IPv4 management address to advertise.

ipv6 *ipv6-address*
: Specifies an IPv6 management address to advertise.

ports
: Advertises configured management address for ports.

all
: Advertises configured management address for all LLDP capable ports.

ethernet *stackid/slot/port*
: Advertises configured management address for the specified Ethernet port.

to *stackid/slot/port*
: Advertises configured management address for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The default mode is used when no addresses are configured to be advertised for a given port. If no management address is explicitly configured to be advertised, the device will use the first available IPv4 address and the first available IPv6 address (so it may advertise IPv4, IPv6 or both). If any addresses are configured to be advertised for a given port, then only those addresses are advertised. If no IP address is configured on any of the above, the port's current MAC address will be advertised.

If a management address is not explicitly configured to be advertised, the device uses the first available IPv4 address and the first available IPv6 address. A Layer 3 switch will select the first available address of each type from those configured on the following types of interfaces, in the following order of preference:

- Physical port on which LLDP will be transmitting the packet.

- Virtual router interface (VE) on a VLAN that the port is a member of
- Dedicated management port
- Loop back interface
- Virtual router interface (VE) on any other VLAN
- Other physical port
- Other interface

For IPv6 addresses, link-local and anycast addresses will be excluded from these searches.

If no IP address is configured on any of the above, the port's current MAC address will be advertised.

The **no** form of the command removes the management IP address.

Examples

The following example shows how to advertise an IPv4 management address.

```
device(config)# lldp advertise management-address ipv4 10.157.2.1 ports ethernet 1/1/4
```

The following example shows how to advertise an IPv6 management address.

```
device(config)# lldp advertise management-address ipv6 2001:DB8::90 ports ethernet 1/1/7
```

lldp advertise max-frame-size

Advertises the maximum frame size capability of the port.

Syntax

lldp advertise max-frame-size ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise max-frame-size ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

The maximum frame size is automatically advertised when LLDP is enabled on a global basis.

The maximum frame size is 1522.

Parameters

ports
Advertises the maximum frame size for ports.

all
Advertises the maximum frame size for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises the maximum frame size for a specific Ethernet port.

to *stackid/slot/port*
Specifies the maximum frame size for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The maximum frame size TLV provides the maximum 802.3 frame size capability of the port. This value is expressed in octets and includes the four-octet Frame Check Sequence (FCS). The default maximum frame size is 1522. The advertised value may change depending on whether the **aggregated-vlan** or **jumbo** commands are configured.

NOTE
On 48GC modules in non-jumbo mode, the maximum size of ping packets is 1486 bytes and the maximum frame size of tagged traffic is no larger than 1581 bytes.

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

Examples

The following example shows how to enable the maximum frame size advertisement.

```
device(config)# lldp advertise max-frame-size ports ethernet 1/1/4 to 1/1/12
```

lldp advertise med-capabilities

Advertises LLDP-MED capabilities information.

Syntax

lldp advertise med-capabilities ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise med-capabilities ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

LLDP-MED information is automatically advertised when LLDP-MED is enabled.

Parameters

ports
Advertises LLDP-MED capabilities information for ports.

all
Advertises LLDP-MED capabilities information for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises LLDP-MED capabilities information for a specific Ethernet port.

to *stackid/slot/port*
Advertises LLDP-MED capabilities information for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The LLDP-MED capabilities advertisement includes the following information:

- The supported LLDP-MED TLVs
- The device type (Network Connectivity device or Endpoint (Class 1, 2, or 3))

NOTE
Disabling the LLDP-MED capabilities disables LLDP-MED.

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

Examples

The following example shows how to enable the LLDP-MED capabilities information advertisement.

```
device(config)# lldp advertise med-capabilities ports ethernet 1/1/1 to 1/1/6
```

lldp advertise med-power-via-mdi

Advertises an Endpoint IEEE 802.3af power-related information. Enables advanced power management between LLDP-MED Endpoints and Network Connectivity Devices.

Syntax

lldp advertise med-power-via-mdi ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise med-power-via-mdi ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

LLDP-MED power-via-MDI information is automatically advertised when LLDP-MED is enabled, the port is a PoE port, and PoE is enabled on the port.

Parameters

ports
: Advertises LLDP-MED power-via-MDI information for a port.

all
: Advertises LLDP-MED power-via-MDI information for all LLDP capable ports.

ethernet *stackid/slot/port*
: Advertises LLDP-MED power-via-MDI information for a specific Ethernet interface.

to *stackid/slot/port*
: Advertises LLDP-MED power-via-MDI information for a range of Ethernet interfaces.

Modes

Global configuration mode

Usage Guidelines

The LLDP-MED Power-via-MDI TLV advertises an Endpoint IEEE 802.3af power-related information, including the following:

- Power type - indicates whether the LLDP-MED device transmitting the LLPDU is a power sourcing device or a powered device.
- Power source - The power source being utilized by a PSE or PD, for example, primary power source, backup power source, or unknown.
- Power priority - The in-line power priority level for the PSE or PD.
- Power level - The total power, in tenths of watts, required by a PD from a PSE, or the total power a PSE is capable of sourcing over a maximum length cable based on its current configuration.

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

Examples

The following example shows how to enable LLDP-MED power-via-MDI information.

```
device(config)# lldp advertise med-power-via-mdi ports ethernet 1/1/1 to 1/1/5
```

lldp advertise port-description

Identifies the port from which the LLDP agent transmitted the advertisement.

Syntax

lldp advertise port-description ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise port-description ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

The port description is automatically advertised when LLDP is enabled on a global basis.

Parameters

ports
Advertises the port description for a port.

all
Advertises the port description for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises the port description for a specific Ethernet port.

to *stackid/slot/port*
Advertises the port description for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

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

The port description is taken from the ifDescr MIB object from MIB-II.

Examples

The following example shows how to enable the port description advertisement.

```
device(config)# lldp advertise port-description ports ethernet 1/1/4 to 1/1/9
```

lldp advertise port-vlan-id

Advertises the Port VLAN Identifier (PVID) that will be associated with untagged or priority-tagged frames.

Syntax

lldp advertise port-vlan-id ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise port-vlan-id ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

The port VLAN ID is automatically advertised when LLDP is enabled on a global basis.

Parameters

ports

Advertises the port VLAN ID for the ports.

all

Advertises the port VLAN ID for all LLDP capable ports.

ethernet *stackid/slot/port*

Advertises the port VLAN ID for a specific Ethernet port.

to *stackid/slot/port*

Advertises the port VLAN ID for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

If the port is not an untagged member of any VLAN (that is, the port is strictly a tagged port), the value zero will indicate that.

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

Examples

The following example shows how to enable port VLAN ID advertisement.

```
device(config)# lldp advertise port-vlan-id ports ethernet 1/1/2 to 1/1/5
```

lldp advertise power-via-mdi

Advertises general information about Power over Ethernet (PoE) capabilities and status of the port.

Syntax

lldp advertise power-via-mdi ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise power-via-mdi ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

The information about PoE capabilities and status of the port is not advertised.

Parameters

ports
Advertises the power-via-MDI information for the port.

all
Advertises the power-via-MDI information for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises the power-via-MDI information for a specific Ethernet port.

to *stackid/slot/port*
Advertises the power-via-MDI information for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The power-via-MDI indicates the following:

- PoE capability (supported or not supported)
- PoE status (enabled or disabled)
- Power Sourcing Equipment (PSE) power pair - indicates which pair of wires is in use and whether the pair selection can be controlled. The Brocade implementation always uses pair A, and cannot be controlled.
- Power class - Indicates the range of power that the connected powered device has negotiated or requested.

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

Examples

The following example shows how to advertise the power-via-MDI information.

```
device(config)# lldp advertise power-via-mdi ports ethernet 1/1/1  to 1/1/10
```

lldp advertise system-capabilities

Advertises the primary functions of the device and indicates whether these primary functions are enabled.

Syntax

lldp advertise system-capabilities ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...] }

no lldp advertise system-capabilities ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...] }

Command Default

The system capabilities are automatically advertised when LLDP is enabled on a global basis.

Parameters

ports
Advertises the system capabilities for the port.

all
Advertises the system capabilities for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises the system capabilities for the specified Ethernet port.

to *stackid/slot/port*
Advertises the system capabilities for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

System capabilities are based on the type of software image in use (Layer 2 switch or Layer 3 router). The enabled capabilities will be the same as the available capabilities, except that when using a router image (base or full Layer 3), if the global route-only feature is turned on, the bridge capability will not be included, since no bridging takes place.

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

Examples

The following example shows how to advertise the system capabilities information.

```
device(config)# lldp advertise system-capabilities ports ethernet 1/1/1  to 1/1/10
```

lldp advertise system-description

Advertises information such as the product name or model number, the version of the system hardware type, the software operating system level, and the networking software version.

Syntax

lldp advertise system-description ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise system-description ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

System description is not advertised.

Parameters

ports
Advertises the system information for ports.

all
Advertises the system information for all LLDP capable ports.

ethernet *stackid/slot/port*
Advertises the system information for a specific Ethernet port.

to *stackid/slot/port*
Advertises the system information for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The system description is the network entity, which can include information such as the product name or model number, the version of the system hardware type, the software operating system level, and the networking software version. The information corresponds to the sysDescr MIB object in MIB-II.

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

Examples

The following example shows how to advertise the system description information.

```
device(config)# lldp advertise system-description ports ethernet 1/1/1 to 1/1/5
```

lldp advertise system-name

Advertises the name assigned to the system.

Syntax

lldp advertise system-name ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp advertise system-name ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

The system name is automatically advertised when LLDP is enabled on a global basis.

Parameters

ports

Advertises the system name for ports.

all

Advertises the system name for all LLDP capable ports.

ethernet *stackid/slot/port*

Advertises the system name for a specific Ethernet port.

to *stackid/slot/port*

Advertises the system name for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The system name is the system administratively assigned name, taken from the sysName MIB object in MIB-II. The sysName MIB object corresponds to the name defined with the CLI command **hostname**.

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

Examples

The following example shows how to advertise the system name information.

```
device(config)# lldp advertise system-name ports ethernet 1/1/1 to 1/1/0
```

lldp enable ports

Enables the receipt and transmission of LLDP packets on ports.

Syntax

lldp enable ports ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp enable ports ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

When LLDP is enabled on a global basis, by default, each port on the Brocade device will be capable of transmitting and receiving LLDP packets.

Parameters

ports
Enables LLDP for a specify port.

all
Enables LLDP for all LLDP capable ports.

ethernet *stackid/slot/port*
Enables LLDP for a specifc Ethernet port.

to *stackid/slot/port*
Enables LLDP for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

When a port is configured to both receive and transmit LLDP packets and the MED capabilities TLV is enabled, LLDP-MED is enabled as well. LLDP-MED is not enabled if the operating mode is set to receive only or transmit only.

The **no** form of the command disables the receipt and transmission of LLDP packets on a port.

Examples

The following example shows how to enable LLDP on a port.

```
device(config)# lldp enable ports ethernet 1/1/1
```

lldp enable receive

Changes the LLDP operating mode from receive and transmit mode to receive only mode.

Syntax

lldp enable receive ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp enable receive ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

When LLDP is enabled on a global basis, each port on the device will be capable of transmitting and receiving LLDP packets.

Parameters

ports

Changes the LLDP operating mode to receive only mode for a specify port.

all

Changes the LLDP operating mode to receive only mode for all LLDP capable ports.

ethernet *stackid/slot/port*

Changes the LLDP operating mode to receive only mode for a specific Ethernet port.

ethernet *stackid/slot/port*

Changes the LLDP operating mode to receive only mode for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command changes the LLDP operating mode to transmit only mode if the device is in both transmit and receive mode and disables the LLDP receive only operating mode if the receive only mode was enabled.

To change the LLDP operating mode to transmit only mode, simply disable the receive mode using the **no lldp enable transmit** command.

NOTE
LLDP-MED is not enabled when you enable the receive only operating mode. To enable LLDP-MED, you must configure the port to both receive and transmit LLDP packets.

NOTE
To change a port LLDP operating mode from transmit only to receive only, first disable the transmit only mode, then enable the receive only mode. If you do not disable the transmit only mode, you will configure the port to both receive and transmit LLDP packets.

Examples

The following example changes a port LLDP operating mode to a receive only mode.

```
device(config)# lldp enable receive ports ethernet 1/1/1 ethernet 1/1/5 ethernet 1/1/7
```

lldp enable snmp med-topo-change-notifications

Enables SNMP notifications and Syslog messages for LLDP-MED topology changes.

Syntax

lldp enable snmp med-topo-change-notifications ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp enable snmp med-topo-change-notifications ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

SNMP notifications and corresponding Syslog messages are disabled.

Parameters

ports
Enables LLDP-MED SNMP notifications and Syslog messages for ports.

all
Enables LLDP-MED SNMP notifications and Syslog messages for all LLDP capable ports.

ethernet *stackid/slot/port*
Enables LLDP-MED SNMP notifications and Syslog messages for a specific Ethernet port.

to *stackid/slot/port*
Enables LLDP-MED SNMP notifications and Syslog messages for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

When you enable LLDP-MED SNMP notifications, corresponding Syslog messages are enabled as well. When you enable LLDP-MED SNMP notifications, the device will send traps and Syslog messages when an LLDP-MED Endpoint neighbor entry is added or removed.

The **no** form of the command disables LLDP-MED SNMP notifications and Syslog messages.

Examples

The following example shows how to enable LLDP-MED SNMP notifications and Syslog messages.

```
device(config)# lldp enable snmp med-topo-change-notifications ports ethernet 1/1/4 to 1/1/6
```

lldp enable snmp notifications

Enables LLDP SNMP notifications and Syslog messages.

Syntax

lldp enable snmp notifications ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp enable snmp notifications ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

LLDP SNMP notifications and corresponding Syslog messages are disabled.

Parameters

ports

Enables LLDP SNMP notifications and Syslog messages for ports.

all

Enables LLDP SNMP notifications and Syslog messages for all LLDP capable ports.

ethernet *stackid/slot/port*

Enables LLDP SNMP notifications and Syslog messages for a specific Ethernet port.

to *stackid/slot/port*

Enables LLDP SNMP notifications and Syslog messages for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

When you enable LLDP SNMP notifications, the device will send traps and corresponding Syslog messages whenever there is a change in the LLDP data received from neighboring devices.

The **no** form of the command disables LLDP SNMP notifications and Syslog messages.

Examples

The following example shows how to enable LLDP SNMP notifications and Syslog messages.

```
device(config)# lldp enable snmp notifications ports ethernet 1/1/1 to 1/1/6
```

lldp enable transmit

Changes the LLDP operating mode to transmit only mode.

Syntax

lldp enable transmit ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp enable transmit ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

When LLDP is enabled on a global basis, each port on the device will be capable of transmitting and receiving LLDP packets.

Parameters

ports

Changes the LLDP operating mode to transmit only mode for ports.

all

Changes the LLDP operating mode to transmit only mode for all LLDP capable ports.

ethernet *stackid/slot/port*

Changes the LLDP operating mode to transmit only mode for the specified Ethernet interface.

to *stackid/slot/port*

Changes the LLDP operating mode to transmit only mode for a range of Ethernet interfaces.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command changes the LLDP operating mode to receive only mode if the device is in both transmit and receive mode and disables the LLDP transmit only operating mode if the transmit only mode was enabled.

NOTE
To change a port LLDP operating mode from receive only to transmit only, first disable the receive only mode, then enable the transmit only mode. If you do not disable the receive only mode, you will configure the port to both receive and transmit LLDP packets.

Examples

The following example shows how to set the LLDP operating mode to transmit mode only.

```
device(config)# no lldp enable receive ports ethernet 1/1/1 ethernet 1/1/8
device(config)# lldp enable transmit ports ethernet 1/1/1 ethernet 1/1/8
```

lldp max-neighbors-per-port

Specifies the maximum number of LLDP neighbors per port.

Syntax

lldp max-neighbors-per-port *value*

no lldp max-neighbors-per-port [*value*]

Command Default

The default number of LLDP neighbors per port is 4.

Parameters

value

Specifies the number of LLDP neighbors for which LLDP data will be retained foreach port. The value can range from 1 to 64. The default value is 4.

Modes

Global configuration mode

Usage Guidelines

You can use the **show lldp** command to view the configuration.

The **no** form of the command removes the configured value and reverts to the default value 4.

Examples

The following example shows how to set the number of LLDP neighbors per port to 6.

```
device(config)# lldp max-neighbors-per-port 6
```

lldp max-total-neighbors

Specifies the maximum number of LLDP neighbors for which LLDP data will be retained for the entire system.

Syntax

lldp max-total-neighbors *value*

no lldp max-total-neighbors *value*

Command Default

The default number of LLDP neighbors per device is 392.

Parameters

value

Specifies the number of LLDP neighbors per device. The value can range from 16 to 8192. The default value is 392.

Modes

Global configuration mode

Usage Guidelines

You can use the **show lldp** command to view the configuration.

The **no** form of the command removes the configured value and reverts to the default value of 392 number of LLDP neighbors.

Examples

The following example shows how to set the number of LLDP neighbors per device to 100.

```
device(config)# lldp max-total-neighbors 100
```

lldp med fast-start-repeat-count

Configures the Link Layer Discovery Protocol Media Endpoint Devices (LLDP-MED) fast start transmit count.

Syntax

lldp med fast-start-repeat-count *value*

no lldp med fast-start-repeat-count [*value*]

Command Default

The device sends three packets at one-second interval.

Parameters

value

Specifies the number of LLDP packets that will be sent during the LLDP-MED fast start period. The value can range from 1 to 10. The default value is 3 packets.

Modes

Global configuration mode

Usage Guidelines

The LLDP-MED fast start repeat count specifies the number of LLDP packets that will be sent during the LLDP-MED fast start period.

The fast start feature enables a Network Connectivity Device to initially advertise itself at a faster rate for a limited time when an LLDP-MED Endpoint has been newly detected or connected to the network. This feature is important within a VoIP network, for example, where rapid availability is crucial for applications such as emergency call service location (E911). The fast start timer starts when a Network Connectivity Device receives the first LLDP frame from a newly detected Endpoint.

NOTE
The LLDP-MED fast start mechanism is only intended to run on links between Network Connectivity devices and Endpoint devices. It does not apply to links between LAN infrastructure elements, including between Network Connectivity devices, or to other types of links.

The **no** form of the command removes the configured value and reverts to the default value of 3 packets per second.

Examples

The following example shows how to set the LLDP-MED fast start transmit count to 6.

```
device(config)# lldp med fast-start-repeat-count 6
```

lldp med location-id civic-address

Configures a configure a civic address-based location for LLDP-MED.

Syntax

lldp med location-id civic-address refers-to *reference* **country** *country-code* { **elem** *CA-type value* [**elem** *CA-type value*] ... | **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] } }

no lldp med location-id civic-address refers-to *elem* **country** *country-code* { **elem** *CA-type value* [**elem** *CA-type value*] ... | **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] } }

Command Default

LLDP-MED civic address is not configured.

Parameters

refers-to *reference*

Specifies what the location the entry refers to. Specify one of the following: **client**, **dhcp-server**, or **network-element**.

NOTE
Where **dhcp-server** or **network-element** should only be used if it is known that the Endpoint is in close physical proximity to the DHCP server or network element.

country *country-code*

Specifies a two-letter ISO 3166 country code in capital ASCII letters. CA - Canada, DE - Germany, JP - Japan, KR - Korea, US - United States.

elem *CA-type*

Specifies the civic address element. The a value from 0 to 255, that describes the civic address element. Refer to the usage guidelines.

value

Specifies the actual value of the elem CA type.

ethernet *stackid/slot/port*

Specifies the Ethernet port.

to *stackid/slot/port*

Specifies a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

If the value of an element contains one or more spaces, use double quotation marks (") at the beginning and end of the string. For example, elem 3 "Santa Clara" .

TABLE 7 Elements used with civic address

Civic Address (CA) type	Description	Acceptable values / examples
0	Language	The ISO 639 language code used for presenting the address information.
1	National subdivisions (state, canton, region, province, or prefecture)	Examples: Canada - Province Germany - State Japan - Metropolis Korea - Province United States - State
2	County, parish, gun (JP), or district (IN)	Examples: Canada - County Germany - County Japan - City or rural area Korea - County United States - County
3	City, township, or shi (JP)	Examples: Canada - City or town Germany - City Japan - Ward or village Korea - City or village United States - City or town
4	City division, borough, city district, ward, or chou (JP)	Examples: Canada - N/A Germany - District Japan - Town Korea - Urban district United States - N/A
5	Neighborhood or block	Examples: Canada - N/A Germany - N/A Japan - City district Korea - Neighborhood United States - N/A
6	Street	Examples: Canada - Street Germany - Street Japan - Block Korea - Street United States - Street

TABLE 7 Elements used with civic address (continued)

Civic Address (CA) type	Description	Acceptable values / examples
16	Leading street direction	N (north), E (east), S (south), W (west), NE, NW, SE, SW
17	Trailing street suffix	N (north), E (east), S (south), W (west), NE, NW, SE, SW
18	Street suffix	Acceptable values for the United States are listed in the United States Postal Service Publication 28 [18], Appendix C. Example: Ave, Place
19	House number	The house number (street address) Example: 1234
20	House number suffix	A modifier to the house number. It does not include parts of the house number. Example: A, 1/2
21	Landmark or vanity address	A string name for a location. It conveys a common local designation of a structure, a group of buildings, or a place that helps to locate the place. Example: UC Berkeley
22	Additional location information	An unstructured string name that conveys additional information about the location. Example: west wing
23	Name (residence and office occupant)	Identifies the person or organization associated with the address. Example: Textures Beauty Salon
24	Postal / zip code	The valid postal / zip code for the address. Example: 95054-1234
25	Building (structure)	The name of a single building if the street address includes more than one building or if the building name is helpful in identifying the location. Example: Law Library
26	Unit (apartment, suite)	The name or number of a part of a structure where there are separate administrative units, owners, or tenants, such as separate companies or families who occupy that structure. Common examples include suite or apartment designations. Example: Apt 27
27	Floor	Example: 4
28	Room number	The smallest identifiable subdivision of a structure. Example: 7A
29	Placetype	The type of place described by the civic coordinates. For example, a home, office, street, or other public space. Example: Office

TABLE 7 Elements used with civic address (continued)

Civic Address (CA) type	Description	Acceptable values / examples
30	Postal community name	When the postal community name is defined, the civic community name (typically CA type 3) is replaced by this value. Example: Alviso
31	Post office box (P.O. box)	When a P.O. box is defined, the street address components (CA types 6, 16, 17, 18, 19, and 20) are replaced with this value. Example: P.O. Box 1234
32	Additional code	An additional country-specific code that identifies the location. For example, for Japan, this is the Japan Industry Standard (JIS) address code. The JIS address code provides a unique address inside of Japan, down to the level of indicating the floor of the building.
128	Script	The script (from ISO 15924 [14]) used to present the address information. Example: Latn **NOTE** If not manually configured, the system assigns the default value **Latn**
255	Reserved	

The **no** form of the command removes the LLDP-MED civic address.

Examples

The following example shows how to configure a civic address-based location.

```
device(config)# lldp med location-id civic-address refers-to client country US elem 1 CA elem 3 "Santa
Clara" elem 6 "4980 Great America Pkwy" elem 24 95054 elem 27 5 elem 28 551 elem 29 office elem 23
"John Doe"
```

lldp med location-id coordinate-based

Configures a coordinate-based location for an Endpoint device.

Syntax

lldp med location-id coordinate-based latitude *degrees* **resolution** *bits* **longitude** *degrees* **resolution** *bits* **altitude** { **floors** *number* **resolution** *bits* | **meters** *number* **resolution** *bits* }*datum* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp med location-id coordinate-based latitude *degrees* **resolution** *bits* **longitude** *degrees* **resolution** *bits* **altitude** { **floors** *number* **resolution** *bits* | **meters** *number* **resolution** *bits* }*datum* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

Coordinate-based location for an Endpoint device is not configured.

Parameters

latitude *degrees*

Specifies the angular distance north or south from the earth equator measured through 90 degrees. Positive numbers indicate a location north of the equator and negative numbers indicate a location south of the equator.

resolution *bits*

Specifies the precision of the value given for latitude. A smaller value increases the area within which the device is located. For latitude, the value can range from 1 to 34.

longitude *degrees*

Specifies the angular distance from the intersection of the zero meridian. Positive values indicate a location east of the prime meridian and negative numbers indicate a location west of the prime meridian.

resolution *bits*

Specifies the precision of the value given for longitude. A smaller value increases the area within which the device is located. For longitude resolution, enter a number between 1 and 34.

altitude

Specifies the vertical elevation of a building above the ground.

floors *number*

Specifies the vertical elevation of a building above the ground, where 0 represents the floor level associated with the ground level at the main entrance and larger values represent floors that are above (higher in altitude) floors with lower values. Sub-floors can be represented by non-integer values.

resolution *bits*

Specifies the precision of the value given for altitude. A smaller value increases the area within which the device is located. For floors resolution, enter the value 0 if the floor is unknown, or 30 if a valid floor is being specified.

meters *number*

Specifies the vertical elevation in number of meters, as opposed to floors.

resolution *bits*

Specifies the precision of the value given for altitude. A smaller value increases the area within which the device is located. For meters resolution, enter a value from 0 to 30.

datum

Specifies the map used as the basis for calculating the location. The value can be one of the following:

wgs84

World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

nad83-navd88

North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). Use this value when referencing locations on land. If land is near tidal water, use nad83-mllw.

nad83-mllw

North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is mean lower low water (MLLW). Use this value when referencing locations on water, sea, or ocean.

ethernet *stackid/slot/port*

Specifies the Ethernet port.

to *stackid/slot/port*

Specifies a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes a coordinate-based location for an Endpoint device.

Examples

The following example shows how to configure a coordinate-based location.

```
device(config)# lldp med location-id coordinate-based latitude -78.303 resolution 20 longitude 34.27
resolution 18 altitude meters 50 resolution 16 wgs84
```

lldp med location-id ecs-elin

Configures an Emergency Call Service (ECS) based location for Link Layer Discovery Protocol Media Endpoint Devices (LLDP-MED).

Syntax

lldp med location-id ecs-elin *numeric-string***ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp med location-id ecs-elin *numeric-string* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Parameters

numeric-string

Specifies the Emergency Location Identification Number (ELIN) from the North America Numbering Plan format, supplied to the Public Safety Answering Point (PSAP) for ECS purposes. The value can range from 10 to 25 digits in length.

ports

Configures Emergency Call Service (ECS) based location for ports.

all

Configures Emergency Call Service (ECS) based location for all LLDP capable ports.

ethernet *stackid/slot/port*

Configures Emergency Call Service (ECS) based location for a specific Ethernet port.

to *stackid/slot/port*

Configures Emergency Call Service (ECS) based location for a range of Ethernet ports.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the configured Emergency Call Service (ECS) based location.

Examples

The following example shows how to configure an ECS-based location for LLDP-MED.

```
device(config)# lldp med location-id ecs-elin 4082071700
```

lldp med network-policy application

Defines an LLDP-MED network policy for an Endpoint.

Syntax

lldp med network-policy application *application-type* **tagged vlan** *vlan-id* **priority** *priority-value* **dscp** *dscp-value* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp med network-policy application *application-type* **tagged vlan** *vlan-id* **priority** *priority-value* **dscp** *dscp-value* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

lldp med network-policy application *application-type* **untagged dscp** *dscp-value* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp med network-policy application *application-type* **untagged dscp** *dscp-value* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

lldp med network-policy application *application-type* **priority-tagged priority** *priority-value* **dscp** *dscp-value* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp med network-policy application *application-type* **priority-tagged priority** *priority-value* **dscp** *dscp-value* **ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

LLDP-MED network policy is not defined.

Parameters

application-type

Configures the primary function of the applications defined by this network policy. Application type can be one of the following:

guest-voice

Limited voice service for guest users and visitors with their own IP telephony handsets or similar devices that support interactive voice services.

guest-voice-signaling

Limited voice service for use in network topologies that require a different policy for guest voice signaling than for guest voice media.

softphone-voice

Softphone voice service for use with multi-media applications that work in association with VoIP technology, enabling phone calls direct from a PC or laptop. Softphones do not usually support multiple VLANs, and are typically configured to use an untagged VLAN or a single tagged data-specific VLAN. Note that when a network policy is defined for use with an untagged VLAN, the Layer 2 priority field is ignored and only the DSCP value is relevant.

streaming-video

Applies to broadcast or multicast-based video content distribution and similar applications that support streaming video services requiring specific network policy treatment. Video applications that rely on TCP without buffering would not be an intended use of this application type.

video-conferencing
Applies to dedicated video conferencing equipment and similar devices that support real-time interactive video/audio services.

video-signaling
For use in network topologies that require a separate policy for video signaling than for video media. Note that this application type should not be advertised if all the same network policies apply as those advertised in the video conferencing policy TLV.

voice
For use by dedicated IP telephony handsets and similar devices that support interactive voice services.

voice-signaling
For use in network topologies that require a different policy for voice signaling than for voice media. Note that this application type should not be advertised if all the same network policies apply as those advertised in the voice policy TLV.

tagged vlan *vlan-id*
Specifies the tagged VLAN that the specified application type will use.

untagged
Configures the device to use an untagged frame format.

priority-tagged
Configures the device to use priority-tagged frames. In this case, the device uses the default VLAN (PVID) of the ingress port.

priority *priority-value*
Configures the Layer 2 priority value to be used for the specified application type. Enter 0 to use the default priority. Valid values are 0 through 7.

dscp *dscp-value*
Configures the Layer 3 Differentiated Service codepoint priority value to be used for the specified application type. Enter 0 to use the default priority. Valid values are 0 through 63.

ports
Specifies the ports.

ethernet *stackid/slot/port*
Configures the network policy on the specified Ethernet interface.

to *stackid/slot/port*
Configures the network policy on a range of Ethernet interfaces.

Modes

Global configuration mode

Usage Guidelines

An LLDP-MED network policy defines an Endpoint VLAN configuration (VLAN type and VLAN ID) and associated Layer 2 and Layer 3 priorities that apply to a specific set of applications on a port.

NOTE
This feature applies to applications that have specific real-time network policy requirements, such as interactive voice or video services. It is not intended to run on links other than between Network Connectivity devices and Endpoints, and therefore does not advertise the multitude of network policies that frequently run on an aggregated link.

The **no** form of the command removes the defined LLDP-MED network policy for an Endpoint.

Examples

The following example shows how to set LLDP-MED network policy for an Endpoint.

```
device(config)# lldp med network-policy application voice tagged vlan 99 priority 3 dscp 22 port
ethernet 1/1/1
```

lldp reinit-delay

Configures the minimum time between port reinitializations.

Syntax

lldp reinit-delay *seconds*

no lldp reinit-delay [*seconds*]

Command Default

When LLDP is enabled, the default time between port reinitializations is set to 2 seconds.

Parameters

seconds

Specifies the time between port reinitializations. The value can range from 1 to 10 seconds. The default is 2 seconds.

Modes

Global configuration mode

Usage Guidelines

The LLDP re-initialization delay timer specifies the minimum number of seconds the device will wait from when LLDP is disabled on a port, until it will honor a request to re-enable LLDP on that port.

The **no** form of the command removes the configured value and reverts the interval between port reinitializations to 2 seconds.

Examples

The following example sets the re-initialization delay timer to 5 seconds.

```
device(config)# lldp reinit-delay 5
```

lldp run

Enables LLDP globally.

Syntax

lldp run

no lldp run

Command Default

LLDP is enabled by default on individual ports.

Modes

Global configuration mode

Usage Guidelines

To enable LLDP on individual ports first LLDP has to be enabled globally (on the entire device).

The **no** form of the command disable LLDP globally.

Examples

The following example shows how to enable LLDP globally.

```
device(config)# lldp run
```

lldp snmp-notification-interval

Configures the minimum time between SNMP traps and Syslog messages.

Syntax

lldp snmp-notification-interval *seconds*

no lldp snmp-notification-interval [*seconds*]

Command Default

The default time between transmission of SNMP traps and Syslog messages is set to 5 seconds.

Parameters

seconds

Configures the transmission time between SNMP traps and Syslog messages. The value can range from 5 to 3600 seconds. The default is 5 seconds.

Modes

Global configuration mode

Usage Guidelines

When SNMP notifications and Syslog messages for LLDP are enabled, the device will send no more than one SNMP notification and corresponding Syslog message within a five second period.

The **no** form of the command removes the configured value and reverts the transmission time between SNMP traps and Syslog messages to 5 seconds.

Examples

The following example shows how to set the minimum time interval between traps and Syslog messages to 60 seconds.

```
device(config)# lldp snmp-notification-interval 60
```

lldp tagged-packets

Enables support for tagged LLDP packets.

Syntax

lldp tagged-packets process

no lldp tagged-packets [**process**]

Command Default

By default, the devices do not accept tagged LLDP packets from other vendors' devices.

Parameters

process

Enables processing of tagged LLDP packets.

Modes

Global configuration mode

Usage Guidelines

When support for tagged LLDP packets is enabled, the device will accept incoming LLDP tagged packets if the VLAN tag matches any of the following:

- a configured VLAN on the port
- the default VLAN for a tagged port
- the configured untagged VLAN for a dual-mode port

The **no** form of the command disables support for tagged LLDP packets.

Examples

The following example enables support for tagged LLDP packets.

```
device(config)# lldp tagged-packets process
```

lldp transmit-delay

Configures the minimum time between LLDP transmissions.

Syntax

lldp transmit-delay *seconds*

no lldp transmit-delay [*seconds*]

Command Default

When LLDP is enabled, the system automatically sets the LLDP transmit delay timer to 2 seconds.

Parameters

seconds

Configures the LLDP transmit delay timer. The value can range from 1 to 8192 seconds. The default value is 2 seconds.

Modes

Global configuration mode

Usage Guidelines

The LLDP transmit delay timer must not be greater than one quarter of the LLDP transmission interval (CLI command **lldp transmit-interval**).

The LLDP transmit delay timer prevents an LLDP agent from transmitting a series of successive LLDP frames during a short time period, when rapid changes occur in LLDP. It also increases the probability that multiple changes, rather than single changes, will be reported in each LLDP frame.

The **no** form of the command removes the configured valie and reverts to the default value of 2 seconds.

Examples

The following example shows how to set the LLDP transmit delay timer to 7 seconds.

```
device(config)# lldp transmit-delay 7
```

lldp transmit-hold

Configures the holdtime multiplier for transmit time to live (TTL).

Syntax

lldp transmit-hold *value*

no lldp transmit-hold [*value*]

Command Default

When LLDP is enabled, the device automatically sets the holdtime multiplier for TTL to four.

Parameters

value

Configures the transmit holdtime multiplier. The value can range from 2 to 10. The default is 4.

Modes

Global configuration mode

Usage Guidelines

The holdtime multiplier for transmit TTL is used to compute the actual time-to-live (TTL) value used in an LLDP frame. The TTL value is the length of time the receiving device maintains the information in its MIB.

NOTE
Setting the transmit interval or transmit holdtime multiplier, or both, to inappropriate values can cause the LLDP agent to transmit LLDPDUs with TTL values that are excessively high. This in turn can affect how long a receiving device will retain the information if it is not refreshed.

The **no** form of the command removes the configured value and sets the holdtime multiplier for TTL to the default value four.

Examples

The following example shows how to set the holdtime multiplier to 6.

```
device(config)# lldp transmit-hold 6
```

lldp transmit-interval

Sets the interval between regular LLDP transmissions.

Syntax

lldp transmit-interval *seconds*

no lldp transmit-interval *seconds*

Command Default

When LLDP is enabled, the LLDP transmit interval between LLDP packet transmissions is set to 30 seconds.

Parameters

seconds

Configures the time interval between LLDP packet transmissions. The value can range from 5 to 32768 seconds.

Modes

Global configuration mode

Usage Guidelines

Setting the transmit interval or transmit holdtime multiplier, or both, to inappropriate values can cause the LLDP agent to transmit LLDPDUs with TTL values that are excessively high. This in turn can affect how long a receiving device will retain the information if it is not refreshed.

The **no** form of the command removes the configured value and sets the time interval between LLDP packet transmissions to 30 seconds.

Examples

The following example shows how to set the time interval between LLDP packet transmissions to 100 seconds.

```
device(config)# lldp transmit-interval 40
```

lldp-pass-through

Enables reception and transmission of Link Layer Discovery Protocol (LLDP) packets over an 802.1x blocked port.

Syntax

lldp-pass-through { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

no lldp-pass-through { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...] }

Command Default

The default behavior is to drop received LLDP packets and not to transmit LLDP packets over an 802.1x disabled port.

Parameters

all

Enables the LLDP processing on all 802.1x blocked ports.

ethernet *stackid/slot/port*

Enables reception and transmission of LLDP packets for specific Ethernet port.

to *stackid/slot/port*

Enables reception and transmission of LLDP packets for a range of Ethernet ports.

Modes

Dot1x configuration mode

Usage Guidelines

This command is supported only on FSX devices.

The default behavior is to drop received LLDP packets and not to transmit LLDP packets over an 802.1x disabled port.

The **no** form of the command disables LLDP processing on 802.1x blocked ports.

Examples

The following example shows how to enable LLDP processing on all 802.1x blocked ports.

```
device(config)# dot1x
device(config-dot1x)# lldp-pass-through all
```

The following example shows how to enable LLDP processing on a specific 802.1x blocked port.

```
device(config)# dot1x
device(config-dot1x)# lldp-pass-through ethernet 1/1/1
```

load-balance symmetric

Enables symmetric load balancing for IPv4 and IPv6 data traffic on Brocade FastIron devices.

Syntax

load-balance symmetric

no load-balance symmetric

Modes

Global configuration mode

Usage Guidelines

This command configuration affects selection of LAG member port after symmetric load balancing is enabled. For a bidirectional (forward and reverse direction) traffic flow, same port in the LAG and/or same next hop for ECMP is chosen.

The **no** form of the command disables symmetric load balancing in the system.

Examples

The following example enables symmetric load balancing for IPv4 and IPv6 data traffic on a Brocade FastIron device.

```
device(config)# load-balance symmetric
```

History

Release version	Command history
8.0.30b	This command was introduced.

local-as

Specifies the BGP autonomous system number (ASN) where the device resides.

Syntax

local-as *num*

no local-as

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.

The ASN for associates a given device it with other devices in its autonomous system.

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-router)# local-as 777
```

local-userdb

Creates a local user database.

Syntax

local-userdb *db-name*

no local-userdb *db-name*

Command Default

No local user databases exists.

Parameters

db-name

Configures the name of the local user database. The name can be up to 31 alphanumeric characters.

Modes

Global configuration mode

Usage Guidelines

Brocade supports a maximum of ten local user databases, each containing up to 50 user records. Each user record consists of a username and password.

The **no** form of the command removes a local database.

Examples

The following example shows how to configure a local user database.

```
device(config)# local-userdb userdb1
device(config-localuserdb-userdb1)#
```

logging

Enables logging on the Router Advertisement (RA) guard policy.

Syntax

logging

no logging

Modes

RA guard policy configuration mode

Usage Guidelines

The **no** form of this command disables logging on the policy.

Logging cannot be modified if the RA guard policy is in use.

You can verify the logs for RA guard, such as RAs dropped, permitted, count for dropped packets, and reasons for the drop.

Logging increases the CPU load and for higher traffic rates, RA packets drop due to congestion if they are received at the line rate. For less load on the CPU, logging can be disabled on the RA guard policy.

Examples

The following example enables logging on an RA guard policy:

```
Brocade(config)# ipv6 raguard policy p1
Brocade(config-ipv6-RAG-policy p1)# logging
```

logging buffered

Enables logging of specific messages or changes the number of entries the local Syslog buffer can store.

Syntax

logging buffered { *level* | *num-entries* }

no logging buffered { *level* | *num-entries* }

Command Default

The number of entries the local Syslog buffer can store is 50.

Parameters

level

Specifies the message level. The level parameter can have one of the following values: **alerts**, **critical**, **debugging**, **emergencies**, **errors**, **informational**, **notifications**, **warnings**.

num-entries

Configures the he number of entries the local Syslog buffer can store. The value can range from 1 to 1000. The number of entries the local Syslog buffer can store is 50.

Modes

Global configuration mode

Usage Guidelines

The software will not log informational or debugging messages.

To change the message level, disable logging of specific message levels. You must disable the message levels on an individual basis.

For logging buffered num-entries

- You must save the configuration and reload the software to place the change into effect.
- If you decrease the size of the buffer, the software clears the buffer before placing the change into effect.
- If you increase the size of the Syslog buffer, the software will clear some of the older locally buffered syslog messages.

The commands in the example below changes the log level to notification messages or higher.

The **no** form of the command with *num-entries* option resets the syslog buffer size to the default of 50 and with the *level* option disables logging of the specified message levels.

Examples

The following example shows how to enable the logging of debugging messages.

```
device(config)# logging buffered debugging
```

The following example shows how to set the number of entries the local Syslog buffer can store to 1000.

```
device(config)# logging buffered 1000
```

logging console

Enables real-time display of Syslog messages.

Syntax

logging console

no logging console

Command Default

To view Syslog messages generated by a device, you need to display the Syslog buffer or the log on a Syslog server used by the device.

Modes

Global configuration mode

Usage Guidelines

To enable display of real-time Syslog messages in Telnet or SSH sessions, you should enable display of real-time Syslog messages within the individual sessions.

You can enter this command from the serial console or a Telnet or SSH session.

You can enable real-time display of Syslog messages on the management console. When you enable this command, the software displays a Syslog message on the management console when the message is generated. However, to enable display of real-time Syslog messages in Telnet or SSH sessions, you also must enable display within the individual sessions.

The **no** form of the command disables real-time display of syslog messages.

Examples

The following example shows how to enable real-time display of Syslog messages.

```
device(config)# logging console
```

logging cli-command

Enables logging of all syntactically valid CLI commands from each user session into the system log.

Syntax

logging cli-command

no logging cli-command

Command Default

Logging of CLI commands is not enabled.

Modes

Global configuration mode

Usage Guidelines

If the **logging cli-command** command is configured, all the CLI commands executed by the user are logged in the system log and are displayed in the **show logging** command output.

The **no** form of the command disables the logging of CLI commands from each user session into the system log.

Examples

The following example enables the logging of CLI commands on the device.

```
device(config)# logging cli-command
```

The following example shows the system log records which are displayed in the **show logging** command output. The system log contains the valid commands that are executed by the user.

```
Brocade (config)#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 5 overruns)
            Buffer logging: level ACDMEINW, 50 messages logged
            level code: A=alert C=critical D=debugging M=emergency E=error I=informational
N=notification W=warning
Dynamic Log Buffer (50 lines):
8d02h28m43s:I:CLI CMD: "ip route 0.0.0.0 0.0.0.0 10.20.64.1" by un-authenticated
user from console
8d02h28m24s:I:System: Interface ethernet 1/1, state up
8d02h28m22s:I:CLI CMD: "enable" by un-authenticated user from console
8d02h28m22s:I:PORT: 1/1 enabled by un-authenticated user from console session
8d02h28m19s:I:CLI CMD: "disable" by un-authenticated user from console
8d02h28m19s:I:PORT: 1/1 disabled by un-authenticated user from console session
8d02h28m16s:I:CLI CMD: "interface ethernet 1/1" by un-authenticated user from
console
```

logging-enable

Enables IPv6 ACL logging.

Syntax

logging-enable

no logging-enable

Command Default

Logging is not enabled.

Modes

IPv6 access list configuration mode

Usage Guidelines

This command is supported only for IPv6 devices. Use the **acl-logging** command for IPv4 devices.

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

Examples

The following example enables ACL logging on an IPv6 device.

```
device(config)# ipv6 access-list ACL_log_v6
device(config-ipv6-access-list ACL_log_v6)# logging-enable
```

logging enable config-changed

Configures a device to generate Syslog messages when the startup-config file is changed.

Syntax

logging enable config-changed

no logging enable config-changed

Command Default

The trap is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the generation of the syslog messages when the startup-config file is changed.

Examples

The following example shows how to enable Syslog messages when the startup-config file is changed.

```
device(config)# logging enable config-changed
```

logging enable rfc5424

Enables Syslog logging in accordance with RFC 5424 which provides the maximum amount of information in every Syslog in a structured format.

Syntax

logging enable rfc5424

no logging enable rfc5424

Command Default

Syslog is generated in accordance with RFC 3164.

Modes

Global configuration mode

Usage Guidelines

The Logging buffer must be cleared before enabling Syslog specific to RFC 5424, otherwise system throws an error.

If the **logging cli-command** command is present in the running configuration, switching between the default RFC 3164 Syslog logging and the RFC 5424-specific Syslog logging is not supported.

The **no** form of the command enables Syslog logging in accordance with RFC 3164.

Examples

The following example enables Syslog logging in accordance with RFC 5424.

```
device(config)# clear logging
device(config)# logging enable rfc5424
```

The following example removes the configuration to enable Syslog logging specific to RFC 5424 and enables Syslog logging in accordance with RFC 3164.

```
device(config)# clear logging
device(config)# no logging enable rfc5424
```

History

Release version	Command history
8.0.40	This command was introduced.
08.0.30h	Support for the command was added.

logging enable user-login

Configures to allow to view the user-login details in the Syslog messages and traps.

Syntax

logging enable user-login

no logging enable user-login

Command Default

User login details in the Syslog messages and traps is not enabled by default.

Modes

Global configuration mode

Usage Guidelines

Brocade devices send Syslog messages and SNMP traps when a user logs into or out of the User EXEC or Privileged EXEC level of the CLI. The feature applies to users whose access is authenticated by an authentication-method list based on a local user account, RADIUS server, or TACACS/TACACS+ server.

The **no** form of the command disables the user log details from the syslog messages and traps.

Examples

The following example shows how enable the view option to view the user log details.

```
device(config)# logging enable user-login
```

logging facility

Configures the log facility to log the messages from the device.

Syntax

logging facility *facility-name*

no logging facility *facility-name*

Command Default

The default facility for messages the device sends to the Syslog server is "user".

Parameters

facility-name

Specifies the facility name where to log the messages from the device. The facility-name can be one of the following:

kern
Kernel messages.

user
Random user-level messages.

mail
Mail system.

daemon
System daemons.

auth
Security or authorization messages.

syslog
Messages generated internally by Syslog.

lpr
Line printer subsystem.

news
Netnews subsystem.

uucp
UUCP subsystem.

sys9
cron/at subsystem.

sys10
Reserved for system use.

sys11
Reserved for system use.

sys12
Reserved for system use.

sys13
Reserved for system use.

sys14
Reserved for system use.

cron
cron/at subsystem.

local0
Reserved for local use.

local1
Reserved for local use.

local2
Reserved for local use.

local3
Reserved for local use.

local4
Reserved for local use.

local5
Reserved for local use.

local6
Reserved for local use.

local7
Reserved for local use.

Modes

Global configuration mode

Usage Guidelines

The Syslog daemon on the Syslog server uses a facility to determine where to log the messages from the Brocade device. You can specify only one facility. If you configure the device to use two Syslog servers, the device uses the same facility on both servers.

The **no** form of the command resets the facility to the default facility.

Examples

The following example shows how to change the log facility.

```
device(config)# logging facility local0
```

logging host

Configures a syslog server.

Syntax

logging host { *ipv4-addr* | *server-name* | **ipv6** *ipv6-addr* } [**udp-port** *number*]

no logging host { *ipv4-addr* | *server-name* | **ipv6** *ipv6-addr* } [**udp-port** *number*]

Command Default

Syslog server is not configured.

Parameters

ipv4-addr
: Configures the server with the specified IPv4 address as the syslog server.

server-name
: Configures the server with the specified name as the syslog server.

ipv6 *ipv6-addr*
: Configures the server with the specified IPv6 saddress as the syslog server.

udp-port *number*
: Specifies the UDP port number.

Modes

Global configuration mode

Usage Guidelines

You can specify up to six syslog servers by configuring the command.

The **no** form of the command removes the syslog server.

Examples

The following example shows how to set the Syslog server with IP address 10.0.0.99.

```
device(config)# logging host 10.0.0.99
```

To specify an additional Syslog server, enter the **logging host** command again.

```
device(config)# logging host 10.0.0.99
```

logging on

Enables local Syslog logging.

Syntax

logging on

no logging on

Command Default

Syslog is enabled by default.

Modes

Global configuration mode

Usage Guidelines

This command enables local Syslog logging with the following defaults:

- Messages of all severity levels (Emergencies - Debugging) are logged.
- Up to 50 messages are retained in the local Syslog buffer.
- No Syslog server is specified.

The **no** form of the command disables local syslog logging.

Examples

The following example shows how to enable local syslog logging.

```
device(config)# logging on
```

logging persistence

Configures the device to save the System log messages after a soft reboot.

Syntax

logging persistence

no logging persistence

Command Default

Logging persistence is not configured.

Modes

Global configuration mode

Usage Guidelines

If the Syslog buffer size was set to a different value using the command **logging buffered**, the System log will be cleared after a soft reboot, even if this feature is enabled. This will occur only with a soft reboot immediately following a Syslog buffer size change. A soft reboot by itself will not clear the System log. To prevent the system from clearing the System log, leave the number of entries allowed in the Syslog buffer unchanged.

Enabling logging persistence does not save Syslog messages after a hard reboot. When the device is power cycled, the Syslog messages are cleared.

If logging persistence is enabled and you load a new software image on the device, you must first clear the log if you want to reload the device.

The **no** form of the command disables the device to save system log messages after a soft reboot.

Examples

The following example shows how to enable the device to save the System log messages after a soft reboot.

```
device(config)# logging persistence
```

login-page

Configures the login page details to redirect the client to the login page hosted on the external captive portal server.

Syntax

login-page *page-name*

no login-page *page-name*

Command Default

Login page for redirecting the client is not configured.

Parameters

page-name

Specifies the login page created on the external captive portal server.

Modes

Captive portal configuration mode

Usage Guidelines

The login page details must be same as the login page hosted on the external captive portal server.

The **no** form of the command removes the login page configuration.

Examples

The following example configures the login page details to redirect the client to the login page hosted on the external captive portal server.

```
device(config)# captive-portal cp_brocade
device(config-cp-cp_brocade)# login-page /guest/brocadeguestlogin.php
```

History

Release version	Command history
8.0.40	This command was introduced.
8.0.30j	This command was added to FastIron 8.0.30j

loop-detection

Enables loop detection on a physical port (Strict Mode) or a VLAN (Loose Mode).

Syntax

loop-detection [**shutdown-disable**]

no loop-detection [**shutdown-disable**]

Command Default

Loop detection is disabled by default.

Parameters

shutdown-disable

Disables shutdown of port due to loop detection.

Modes

Interface configuration mode

VLAN configuration mode

Usage Guidelines

By default, the port will send test packets every one second, or the number of seconds specified by the **loop-detection-interval** command.

The **no** form of the command disables loop detection.

Examples

The following example shows how to enable loop-detection on a physical port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# loop-detection
```

The following example shows how to enable loop-detection on a VLAN.

```
device(config)# vlan 20
device(config-vlan-20)# loop-detection
```

loop-detection-interval

Configures the time interval of how often a test packet is sent on a port.

Syntax

loop-detection-interval *number*

no loop-detection-interval *number*

Command Default

Loop detection time is set to 1 second.

Parameters

number

Specifies a value from 1 to 100 seconds. The system multiplies the entry by 0.1 to calculate the interval at which test packets will be sent.

Modes

Global configuration mode

Usage Guidelines

When loop detection is enabled, the loop detection time unit is 0.1 second, with a default of 10 (one second). The range is from 1 (one tenth of a second) to 100 (10 seconds). You can use the **show loop-detection status** command to view the loop detection interval.

The **no** form of the command sets the loop detection interval to the default global loop detection interval of 1 second.

Examples

The following example shows how to set the loop detection interval to 5 seconds (50*0.1).

```
device(config)# loop-detection-interval 50
```

loop-detection shutdown-disable

Disables shutdown of a port when a loop detection probe packet is received on an interface.

Syntax

loop-detection shutdown-disable

no loop-detection shutdown-disable

Command Default

Loop detection shutdown is enabled on the interface.

Modes

Interface configuration

Usage Guidelines

The **no** form of this command disables loop detection shutdown.

Shutdown prevention for loop-detect functionality allows users to disable shut down of a port when the loop detection probe packet is received on an interface. This provides control over deciding which port is allowed to enter in to an error-disabled state and go into a shutdown state when a loop is detected.

Examples

The following example disables loop detection shutdown on an interface.

```
device(config)# interface ethernet 1/7
device(config-if-e1000-1/7)# loop-detection shutdown-disable
```

History

Release version	Command history
08.0.20	This command was introduced.

loop-detection-syslog-interval

Specifies the interval (in minutes) at which a syslog is generated.

Syntax

loop-detection-syslog-interval *num*

no loop-detection-syslog-interval *num*

Command Default

The syslog interval is 5 minutes.

Parameters

num

Specifies the syslog interval in minutes. The interval can range from 1 through 1440 minutes.

Modes

Global configuration

Usage Guidelines

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

You can specify the interval at which the loop detection syslog message is generated if the **loop-detection-shutdown-disable** command is configured for the port. This configuration applies to all the ports that have loop detection shutdown prevention configured.

Examples

The following example shows the loop detection syslog interval set to 1 hour.

```
device(config)# loop-detection-syslog-interval 60
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-age-time

Configures the MAC address age timer.

Syntax

mac-age-time *seconds*

no mac-age-time *seconds*

Command Default

The default MAC address age timeout is 300 seconds.

Parameters

seconds

Timeout value in seconds. The timeout value for FCX devices is 0 (disabled) or from 10 through 1,000 seconds. The timeout value for FSX devices, the ICX 7450, and the ICX 7750 is 0 (disabled) or from 10 through 86,400 seconds. The timeout value for the ICX 6430 and ICX 6450 is 0 (disabled) or from 10 through 570 seconds. The timeout value for the ICX 6650 is 0 (disabled) or from 10 through 600 seconds.

Modes

Global configuration mode

Usage Guidelines

To disable the MAC address age timer, set the timeout value to 0.

If the total number of MAC addresses in the system is more than 16, 000, Brocade recommends a MAC address age timer greater than 60 seconds. If the total number of MAC addresses in the system is more than 64, 000, Brocade recommends a MAC address age timer greater than 120 seconds.

Usually, the actual MAC address age time is from one to two times the configured value. For example, if you set the MAC address age timer to 60 seconds, learned MAC address entries age out after remaining unused for between 60 and 120 seconds. However, if all of the following conditions are met, then the MAC address entries age out after a longer than expected duration:

- The MAC address age timer is set to greater than 630 seconds.
- The number of MAC address entries is over 6, 000.
- All MAC address entries are learned from the same packet processor.
- All MAC address entries age out at the same time.

The **no** form of the command resets the MAC address age timeout value to the default value.

Examples

The following example configures the MAC address age timeout to 570 seconds.

```
device(config)# mac-age-time 570
```

mac-authentication apply-mac-auth-filter

Applies the MAC address filter that is configured to exclude the specified MAC address from MAC authentication on a specific interface.

Syntax

mac-authentication apply-mac-auth-filter *filter-id*

no mac-authentication apply-mac-auth-filter *filter-id*

Command Default

The MAC address filters are not configured.

Parameters

filter-id

Specifies the ID of the MAC address filter.

Modes

Interface configuration mode

Usage Guidelines

The filtered MAC addresses are considered pre-authenticated and are not subject to RADIUS authentication.

The MAC address filter must be configured when the RADIUS server itself is connected to an interface where MAC authentication is enabled. If a MAC address filter is not configured for the MAC address of the RADIUS server and applied on the interface, the RADIUS authentication process fails because the device drops all packets from the RADIUS server itself.

The **no** form of the command removes the MAC address filter configuration applied on the specified interface.

Examples

The following example applies the MAC address filter on an interface so that the specified MAC address is excluded from MAC authentication.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication apply-mac-auth-filter 1
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication auth-fail-action

Configures the action to be performed when RADIUS authentication for a MAC address fails.

Syntax

mac-authentication auth-fail-action { **block-traffic** | **restrict-vlan** *vlan-id* }

no mac-authentication auth-fail-action { **block-traffic** | **restrict-vlan** *vlan-id* }

Command Default

Traffic from non-authenticated MAC addresses is blocked.

Parameters

block-traffic

Blocks traffic from non-authenticated MAC addresses.

restrict-vlan

Moves the port on which the traffic was received to a restricted VLAN.

vlan-id

Specifies the ID of the restricted VLAN.

Modes

Interface configuration mode

Global configuration mode

Usage Guidelines

If the ID for the restricted VLAN is not specified at the interface level, the global restricted VLAN ID applies for the interface.

The **no** form of the command disables the authentication failure action.

Examples

The following example configures the device to drop traffic from non-authenticated MAC addresses in hardware.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication auth-fail-action block-traffic
```

The following example configures the device to move the port to a restricted VLAN when MAC authentication fails.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication auth-fail-action restrict-vlan 100
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication auth-fail-dot1x-override

Configures the device to perform 802.1X authentication when a device fails MAC authentication.

Syntax

mac-authentication auth-fail-dot1x-override

no mac-authentication auth-fail-dot1x-override

Modes

Global configuration mode

Examples

The following example configures the device to perform 802.1X authentication when a device fails MAC authentication.

```
device(config)# mac-authentication auth-fail-dot1x-override
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication auth-fail-vlan-id

Configures a specific VLAN as the restricted VLAN for all ports on the device to place the client port when MAC authentication fails.

Syntax

mac-authentication auth-fail-vlan-id *vlan-id*

no mac-authentication auth-fail-vlan-id *vlan-id*

Command Default

The restricted VLAN is not configured.

Parameters

vlan-id

Specifies the VLAN ID of the VLAN to be used as the restricted VLAN.

Modes

Global configuration mode

Usage Guidelines

The **mac-authentication auth-fail-vlan-id** command applies globally to all MAC-authentication-enabled interfaces.

The restricted VLAN must already exist on the device. If the port is a tagged or dual-mode port, you cannot use a restricted VLAN as the authentication failure action.

When an authentication fails, the port can be moved to a configured restricted VLAN instead of failing the client completely. The port is moved to the configured restricted VLAN only if the authentication failure action is set to place the port in a restricted VLAN using the **mac-authentication auth-fail-action** command.

The **no** form of the command removes the restricted VLAN configuration on the VLAN.

Examples

The following example specifies VLAN 200 as the restricted VLAN for all ports on the device.

```
device(config)# mac-authentication auth-fail-vlan-id 200
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, Brocade ICX 7750, and Brocade ICX 7450.

mac-authentication auth-filter

Applies the specified filter on the interface and the MAC addresses defined in the filter (MAC filter) do not have to go through authentication.

Syntax

mac-authentication auth-filter *filter-id vlan-id*

no mac-authentication auth-filter *filter-id vlan-id*

Command Default

There are no filters applied on the interface.

Parameters

filter-id

Specifies the identification number of the filter to be applied on the interface.

vlan-id

Specifies the identification number of the VLAN to which the filter is applied.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command disables this functionality.

A client can be authenticated in an untagged VLAN or tagged VLAN using the MAC address filter for MAC authentication. If auth-filter has tagged VLAN configuration, the clients are authenticated in auth-default VLAN and tagged VLAN provided in auth-filter. The clients authorized in auth-default VLAN allow both untagged and tagged traffic.

If the VLAN is not specified in the command, the auth-default VLAN is used.

Examples

The following example applies the MAC address filter on VLAN 2.

```
device(config)# authentication
device(config-authen)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# mac-auth auth-filter 1 2
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-authentication auth-passwd-format

Specifies the format of the MAC addresses sent to the RADIUS server during MAC authentication.

Syntax

mac-authentication auth-passwd-format { **xx-xx-xx-xx-xx-xx** | **xxxx.xxxx.xxxx** | **xxxxxxxxxxxx** }

no mac-authentication auth-passwd-format { **xx-xx-xx-xx-xx-xx** | **xxxx.xxxx.xxxx** | **xxxxxxxxxxxx** }

Command Default

The MAC address is sent to the RADIUS server in the format xxxxxxxxxxxx.

Parameters

xx-xx-xx-xx-xx-xx

Specifies to send the MAC address to the RADIUS server in the format xx-xx-xx-xx-xx-xx.

xxxx.xxxx.xxxx

Specifies to send the MAC address to the RADIUS server in the format xxx.xxx.xxx.

xxxxxxxxxxxx

Specifies to send the MAC address to the RADIUS server in the format xxxxxxxxxxxx.

Modes

Global configuration mode

Usage Guidelines

When MAC authentication is configured, the Brocade device authenticates MAC addresses by sending username and password information to a RADIUS server. The username and password are used as the MAC address itself; that is, the device uses the MAC address for both the username and the password in the request sent to the RADIUS server.

The **no** form of the command reinstates the default format xxxxxxxxxxxx.

Examples

The following example configures the device to send the MAC address to the RADIUS server in the format xx-xx-xx-xx-xx-xx.

```
device(config)# mac-authentication auth-passwd-format xx-xx-xx-xx-xx-xx
```

The following example configures the device to send the MAC address to the RADIUS server in the format xxxx.xxxx.xxxx.

```
device(config)# mac-authentication auth-passwd-format xxxx.xxxx.xxxx
```

The following example configures the device to send the MAC address to the RADIUS server in the format xxxxxxxxxxxx.

```
device(config)# mac-authentication auth-passwd-format xxxxxxxxxxxx
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication auth-timeout-action

Configures the RADIUS timeout behavior to bypass MAC authentication and permit or deny user access to the network.

Syntax

mac-authentication auth-timeout-action { **failure** | **success** }

no mac-authentication auth-timeout-action { **failure** | **success** }

Command Default

The device resets the authentication process and retries to authenticate the user.

Parameters

failure

Bypasses the authentication process and blocks user access to the network, unless it is specified to move the user to the restricted VLAN using the **mac-authentication auth-fail-action** command, in which case, the user is placed into a VLAN with restricted or limited access.

success

Bypasses the authentication process and permits user access to the network.

Modes

Interface configuration mode

Usage Guidelines

If you configure to move the user to the restricted VLAN using the **mac-authentication auth-fail-action** command along with **mac-authentication auth-timeout-action failure**, the user will be placed into a VLAN with restricted or limited access.

The **no** form of the command resets the RADIUS timeout behavior to retry.

Examples

The following example configures the RADIUS timeout behavior to bypass MAC authentication and block user access to the network.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# mac-authentication auth-timeout-action failure
```

The following example configures the RADIUS timeout behavior to bypass MAC authentication and permit user access to the network.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# mac-authentication auth-timeout-action success
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication clear-mac-session

Clears the MAC authentication MAC session for an address learned on a specific interface.

Syntax

mac-authentication clear-mac-session *mac-address*

Parameters

mac-address

Specifies the MAC address from which the MAC authentication MAC sessions are to be cleared.

Modes

Interface configuration mode

Usage Guidelines

In a configuration with MAC authentication and 802.1X authentication on the same port, the **mac-authentication clear-mac-session** command clears the MAC session, as well as its respective 802.1X session, if it exists.

Examples

The following example clears the MAC authentication MAC session for an address learned on a specific interface.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication clear-mac-session 0000.0034.abd4
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication disable-aging

Disables aging for all MAC addresses subject to authentication on all interfaces or for those learned on a specific interface where MAC authentication is enabled.

Syntax

mac-authentication disable-aging [**denied-mac-only** | **permitted-mac-only**]

no mac-authentication disable-aging [**denied-mac-only** | **permitted-mac-only**]

Command Default

MAC addresses that are authenticated or denied by a RADIUS server are aged out if no traffic is received from the MAC address for a certain period of time.

Parameters

denied-mac-only

Prevents denied sessions from being aged out, but ages out permitted sessions.

permitted-mac-only

Prevents permitted (authenticated and restricted) sessions from being aged out and ages denied sessions.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

Authenticated MAC addresses or non-authenticated MAC addresses that are placed in the restricted VLAN are aged out if no traffic is received from the MAC address within the normal MAC aging interval of the device.

Non-authenticated MAC addresses that are blocked by the device are aged out if no traffic is received from the address over hardware aging period, plus a configurable software aging period.

The **no** form of the command enables aging for all MAC addresses subject to authentication on all interfaces or for those learned on a specific interface where MAC authentication is enabled.

Examples

The following example disables aging for all MAC addresses subject to authentication on all interfaces where MAC authentication is enabled.

```
device(config)# mac-authentication disable-aging
```

The following example disables aging for all MAC addresses subject to authentication on a specific interface.

```
device(config)# interface e 3/1
device(config-if-e1000-3/1)# mac-authentication disable-aging
```

The following example disables denied sessions from being aged out on all interfaces.

```
device(config)# mac-authentication disable-aging denied-mac-only
```

The following example disables permitted (authenticated and restricted) sessions from being aged out on all interfaces.

```
device(config)# mac-authentication disable-aging permitted-mac-only
```

The following example disables denied sessions from being aged out on a specific interface.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication disable-aging denied-mac-only
```

The following example disables permitted sessions from being aged out on a specific interface.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication disable-aging permitted-mac-only
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication disable-ingress-filtering

Disables ingress filtering on non-member VLAN ports.

Syntax

mac-authentication disable-ingress-filtering

no mac-authentication disable-ingress-filtering

Command Default

Ingress filtering is enabled.

Modes

Interface configuration mode

Usage Guidelines

By default, the Brocade device drops tagged packets that are received on non-member VLAN ports. Because the MAC address of the packets is not learned, authentication does not take place. The Brocade device can authenticate clients that send tagged packets on non-member VLAN ports. This enables the Brocade device to add the VLAN dynamically. You can enable dynamic VLAN support for tagged packets on non-member VLAN ports using the **mac-authentication disable-ingress-filtering** command.

The dynamic VLAN support for tagged packets on non-member VLAN ports works only in conjunction with MAC authentication with dynamic VLAN assignment.

The port on which ingress filtering is disabled must be tagged to a VLAN.

The **mac-authentication disable-ingress-filtering** command is not available on the Brocade ICX 6610, Brocade ICX 6450, and Brocade FCX Series.

The **no** form of the command re-enables ingress filtering on non-member VLAN ports.

Examples

The following example disables ingress filtering on non-member VLAN ports.

```
device(config)# interface ethernet 3/1
device(config-if-e100-3/1)# mac-authentication disable-ingress-filtering
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication dos-protection

Enables protection against Denial of Service (DoS) attacks by specifying the maximum rate for RADIUS authentication attempts.

Syntax

mac-authentication dos-protection { **enable** | **mac-limit** *number* }

no mac-authentication dos-protection { **enable** | **mac-limit** *number* }

Command Default

DoS protection is disabled.

Parameters

enable

Enables DoS protection with the default value of 512 as the maximum number for RADIUS authentication attempts.

mac-limit

Configures the maximum number of RADIUS authentication attempts per second beyond which the device disables the port suspecting a DoS attack.

number

Specifies the maximum number of RADIUS authentication attempts allowed per second. The value range can be from 1 through 65535. The default value is 512 authentication attempts per second.

Modes

Interface configuration mode

Usage Guidelines

When DoS protection is enabled, if the number of RADIUS authentication attempts for MAC addresses learned on an interface per second exceeds a configurable rate (by default, 512 authentication attempts per second), the device considers this a possible DoS attack and disables the port. The port must be re-enabled manually.

The **no** form of the command disables DoS protection.

Examples

The following example enables DoS protection.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication dos-protection enable
```

The following example configures the maximum number of RADIUS authentication attempts allowed per second as 520 beyond which the device disables the port suspecting a DoS attack.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication dos-protection mac-limit 520
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication dot1x-override

Configures the device to perform 802.1X authentication when MAC authentication fails when the authentication sequence is configured as MAC authentication followed by 802.1X authentication.

Syntax

mac-authentication dot1x-override

no mac-authentication dot1x-override

Command Default

802.1X authentication is not performed when MAC authentication fails.

Modes

Authentication configuration mode

Usage Guidelines

This command is applicable only when the authentication sequence is configured as MAC authentication followed by 802.1X authentication.

If the **mac-authentication dot1x-override** command is configured, the clients that failed MAC authentication undergoes 802.1X authentication if the failure action is configured as restricted VLAN.

The **no** form of the command disables MAC authentication dot1x override functionality.

Examples

The following example enables MAC authentication dot1x override when MAC authentication fails.

```
device(config)# authentication
device(config-authen)# mac-authentication dot1x-override
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-authentication enable

Enables MAC authentication on all interfaces at once, on individual interfaces, or on a range of interfaces.

Syntax

mac-authentication enable { **all** | **ethernet** *slot/port* [[**to** *slot/port*] [**ethernet** *slot/port*]...] }

no mac-authentication enable { **all** | **ethernet** *slot/port* [[**to** *slot/port*] [**ethernet** *slot/port*]...] }

Command Default

MAC authentication is disabled.

Parameters

all

Specifies to enable MAC authentication on all interfaces on the device.

ethernet *slot/port*

Specifies a specific interface on which MAC authentication must be enabled.

to *slot/port*

Specifies the range of interfaces on which MAC authentication must be enabled.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

In interface configuration mode, the options **all**, **to**, and **ethernet** *slot/port* are not available. You can specify an individual interface or range of interfaces on which you want to enable multi-device authentication as you enter interface configuration mode.

The **no** form of the command disables MAC authentication.

Examples

The following example enables MAC authentication on all interfaces on the device.

```
device(config)# mac-authentication enable all
```

The following example enables MAC authentication on interface 3/1.

```
device(config)# mac-authentication enable ethernet 3/1
```

The following example enables MAC authentication on a range of interfaces.

```
device(config)# mac-authentication enable ethernet 3/1 to 3/6
```

The following example enables MAC authentication on a specific interface.

```
device(config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication enable
```

History

Release version	Command history
08.0.20	This command was replaced on Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750 by the **mac-authentication enable (Flexible authentication)** command.

mac-authentication enable (Flexible authentication)

Enables MAC authentication globally or on a specific interface.

Syntax

mac-authentication enable [**all** | **ethernet** *device/slot/port*]

no mac-authentication enable [**all** | **ethernet** *device/slot/port*]

Command Default

MAC authentication is not enabled.

Parameters

all

Enables MAC authentication on all interfaces.

ethernet *device/slot/port*

Enables MAC authentication on a specific interface.

Modes

Authentication configuration mode

Usage Guidelines

The **mac-authentication enable** command without any options initializes MAC authentication feature globally. The **mac-authentication enable** command with the **all** or **ethernet** options, enables MAC authentication on all or a specific interface respectively. After initializing MAC authentication feature using the **mac-authentication enable** command, you must enable MAC authentication on all or a specific interface.

The **no** form of the command disables MAC authentication.

Examples

The following example globally enables MAC authentication.

```
device(config)# authentication
device(config-authen)# mac-authentcation enable
device(config-authen)# mac-authentication enable all
```

The following example enables MAC authentication on an interface.

```
device(config)# authentication
device(config-authen)# mac-authentcation enable
device(config-authen)# mac-authentication enable ethernet 1/1/11
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-authentication enable-dynamic-vlan

Enables dynamic VLAN assignment on a MAC authentication-enabled interface to move the port into a VLAN specified by Radius dynamic VLAN attribute.

Syntax

mac-authentication enable-dynamic-vlan

no mac-authentication enable-dynamic-vlan

Command Default

Dynamic VLAN assignment is not enabled.

Modes

Interface configuration mode

Usage Guidelines

To enable dynamic VLAN assignment for authenticated MAC addresses, you must add attributes to the profile for the MAC address on the RADIUS server, and then enable dynamic VLAN assignment on MAC authentication-enabled interfaces.

The **no** form of the command disables dynamic VLAN assignment on a MAC authentication-enabled interface.

Examples

The following example enables dynamic VLAN assignment on a MAC authentication-enabled interface.

```
device(config)# interface e 1/1/1
device(config-if-e1000-1/1/1)# mac-authentication enable-dynamic-vlan
```

History

Release version	Command history
08.0.20	This command was deprecated on Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750 devices.
08.0.30b	This command was reintroduced on Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750 devices. This command was introduced on Brocade ICX 7450 and Brocade ICX 7250 devices.
08.0.30d	This command was deprecated on Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, Brocade ICX 7750, Brocade ICX 7450, and Brocade ICX 7250 devices.

mac-authentication hw-deny-age

Changes the hardware aging period for blocked MAC addresses.

Syntax

mac-authentication hw-deny-age *number*

no mac-authentication hw-deny-age *number*

Command Default

The default time is 70 seconds.

Parameters

num

Specifies the time duration after which the blocked MAC addresses are aged out. Valid values are from 1 through 65535 seconds. The default value is 70 seconds.

Modes

Global configuration mode

Usage Guidelines

On FastIron X Series devices, the hardware aging period for blocked MAC addresses is not fixed at 70 seconds. The hardware aging period for blocked MAC addresses is equal to the length of time specified with the **mac-age-time** command.

On FastIron devices, the hardware aging period for blocked MAC addresses is fixed at 70 seconds and is not configurable. (The hardware aging period for non-blocked MAC addresses is the length of time specified with the **mac-age-time** command.)

The **no** form of the command sets the time to the default value (70 seconds).

Examples

The following example configures the time duration as 10 seconds, after which the blocked MAC address is aged out.

```
device(config)# mac-authentication hw-deny-age 10
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication max-accepted-session

Limits the number of successfully authenticated MAC addresses accepted on a port that has MAC authentication enabled.

Syntax

mac-authentication max-accepted-session *session-number*

no mac-authentication max-accepted-session *session-number*

Parameters

session-number

Specifies the maximum number of successfully authenticated MAC addresses accepted on a specific port. Valid values are from 1 through 250.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables the limitation set on the port for accepting successfully authenticated MAC addresses.

Examples

The following example sets the maximum limit for the number of successfully authenticated MAC addresses accepted on a port as 5.

```
device (config)# interface ethernet 3/11
device(config-if-e1000-3/11)# mac-authentication max-accepted-session 5
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication max-age

Configures the software aging period for multi-device port authentication of a blocked client after which the associated MAC address is aged out.

Syntax

mac-authentication max-age *time*

no mac-authentication max-age *time*

Command Default

The default time is 120 seconds.

Parameters

time

Specifies the software aging period for multi-device port authentication of a blocked client after which the associated MAC address is aged out. Valid values are from 1 through 65535 seconds. The default value is 120 seconds.

Modes

Global configuration mode

Usage Guidelines

After the software aging period ends, the blocked client MAC address ages out, and can be authenticated again if the Brocade device receives traffic from the client MAC address.

The **no** form of the command resets the software aging period to the default value (120 seconds).

Examples

The following example configures the software aging period for multi-device port authentication of a blocked client after which the associated MAC address is aged out.

```
device(config)# mac-authentication max-age 180
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication move-back-to-old-vlan

Specifies the VLAN to which a port must be moved after its RADIUS-specified VLAN assignment expires.

Syntax

mac-authentication move-back-to-old-vlan { **port-configured-vlan** | **port-restrict-vlan** | **system-default-vlan** }

no mac-authentication move-back-to-old-vlan { **port-configured-vlan** | **port-restrict-vlan** | **system-default-vlan** }

Command Default

The port is moved to the VLAN where it was originally assigned after its RADIUS-specified VLAN assignment expires.

Parameters

port-configured-vlan
Removes the port from its RADIUS-assigned VLAN and places it back in the VLAN where it was originally assigned.

port-restrict-vlan
Removes the port from its RADIUS-assigned VLAN and places it in the restricted VLAN.

system-default-vlan
Removes the port from its RADIUS-assigned VLAN and places it in the default VLAN.

Modes

Interface configuration mode

Usage Guidelines

When a MAC session is deleted, if the port is moved back to a VLAN that is different from the running-config file, the system will update the running-config file to reflect the changes. This will occur even if **mac-authentication save-dynamicvlan-to-config** is not configured.

The **no** form of the command reinstates the default behavior of moving the port back to the VLAN where it was originally assigned.

Examples

The following example specifies that the port must be moved back to the VLAN where it was originally assigned after its RADIUS-specified VLAN assignment expires.

```
device (config)# interface ethernet 3/11
device(config-if-e1000-3/11)# mac-authentication move-back-to-old-vlan port-configured-vlan
```

The following example specifies that the port must be moved to a restricted VLAN after its RADIUS-specified VLAN assignment expires.

```
device (config)# interface ethernet 3/11
device(config-if-e1000-3/11)# mac-authentication move-back-to-old-vlan port-restrict-vlan
```

The following example specifies that the port must be moved to the default VLAN after its RADIUS-specified VLAN assignment expires.

```
device (config)# interface ethernet 3/11
device(config-if-e1000-3/11)# mac-authentication move-back-to-old-vlan system-default-vlan
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication no-override-restrict-vlan

Configures a port to remain in the restricted VLAN after a successful MAC authentication.

Syntax

mac-authentication no-override-restrict-vlan

no mac-authentication no-override-restrict-vlan

Command Default

The port moves out of the restricted VLAN to the RADIUS-specified VLAN.

Modes

Interface configuration mode

Usage Guidelines

When the **mac-authentication no-override-restrict-vlan** command is issued, if the RADIUS-specified VLAN configuration is tagged (for example, T:1024) and the VLAN is valid, then the port is placed in the RADIUS-specified VLAN as a tagged port and left in the restricted VLAN. If the RADIUS-specified VLAN configuration is untagged (for example, U:1024), the configuration from the RADIUS server is ignored, and the port is left in the restricted VLAN.

If you configure dynamic VLAN assignment on a MAC authentication-enabled interface, and the Access-Accept message returned by the RADIUS server contains a Tunnel-Type and Tunnel-Medium-Type, but does not contain a Tunnel-Private-Group-ID attribute, then it is considered an authentication failure, and the configured authentication failure action is performed for the MAC address.

If the vlan-name string in the Access-Accept message does not match either the name or the ID of a VLAN configured on the device, then it is considered an authentication failure, and the configured authentication failure action is performed for the MAC address.

For tagged or dual-mode ports, if the VLAN ID provided by the RADIUS server does not match the VLAN ID in the tagged packet that contains the authenticated MAC address as its source address, then it is considered an authentication failure, and the configured authentication failure action is performed for the MAC address.

If an untagged port had previously been assigned to a VLAN through dynamic VLAN assignment, and then another MAC address is authenticated on the same port, but the RADIUS Access-Accept message for the second MAC address specifies a different VLAN, then it is considered an authentication failure for the second MAC address, and the configured authentication failure action is performed. Note that this applies only if the first MAC address has not yet aged out. If the first MAC address has aged out, then dynamic VLAN assignment works as expected for the second MAC address.

For dual mode ports, if the RADIUS server returns T:vlan-name, the traffic will still be forwarded in the statically assigned PVID. If the RADIUS server returns U:vlan-name, the traffic will not be forwarded in the statically assigned PVID.

The **no** form of the command configures the port to move out of the restricted VLAN into the RADIUS-specified VLAN.

Examples

The following example configures a port to remain in the restricted VLAN after a successful MAC authentication.

```
device (config)# interface ethernet 3/1
device(config-if-e1000-3/1)# mac-authentication no-override-restrict-vlan
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication password-format

Configures the MAC authentication password format.

Syntax

mac-authentication password-format { **xx-xx-xx-xx-xx-xx** | **xxxx.xxxx.xxxx** | **xxxxxxxxxxxx** } [**upper-case**]

no mac-authentication password-format { **xx-xx-xx-xx-xx-xx** | **xxxx.xxxx.xxxx** | **xxxxxxxxxxxx** } [**upper-case**]

Command Default

By default, the MAC address is sent to the RADIUS server in the format xxxxxxxxxxxx in lower case.

Parameters

xx-xx-xx-xx-xx-xx

Specifies the MAC authentication password format as xx-xx-xx-xx-xx-xx.

xxxx.xxxx.xxxx

Specifies the MAC authentication password format as xxxx.xxxx.xxxx.

xxxxxxxxxxxx

Specifies the MAC authentication password format as xxxxxxxxxxxx.

upper-case

Converts the password to uppercase.

Modes

Authentication configuration mode

Usage Guidelines

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

You can configure the device to send the MAC address to the RADIUS server in the format xx-xx-xx-xx-xx-xx, xxxx.xxxx.xxxx, or xxxxxxxxxxxx. Use the **upper-case** password format option to send the password in uppercase.

Examples

The following example configures the MAC authentication password format as xx-xx-xx-xx-xx-xx.

```
device(config)# authentication
device(config-authen)# mac-authentication password-format xx-xx-xx-xx-xx-xx
```

The following example configures the MAC authentication password format as xx-xx-xx-xx-xx-xx in upper case.

```
device(config)# authentication
device(config-authen)# mac-authentication password-format xx-xx-xx-xx-xx-xx upper-case
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20c	The **upper-case** option was added.

mac-authentication mac-filter

Configures MAC address filters to exclude the specified MAC address from MAC authentication.

Syntax

mac-authentication mac-filter { *filter-id* } { *mac-address* }

no mac-authentication mac-filter { *filter-id* } { *mac-address* }

Command Default

The MAC address filters are not configured.

Parameters

filter-id

Specifies an ID for the MAC address filter.

mac-address

Specifies the MAC address that must be excluded from MAC authentication.

Modes

Global configuration mode

Usage Guidelines

The filtered MAC addresses are considered pre-authenticated, and are not subject to RADIUS authentication.

A MAC address filter must be configured when the RADIUS server itself is connected to an interface where MAC authentication is enabled. If a MAC address filter is not configured for the MAC address of the RADIUS server and applied on the interface, the RADIUS authentication process fails because the device drops all packets from the RADIUS server itself.

The **no** form of the command removes the MAC address filter configuration and the MAC address is included for MAC authentication.

Examples

The following example configures a MAC address filter 1 for address 0000.0058.aca4.

```
device(config)# mac-authentication mac-filter 1 0000.0058.aca4
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-authentication password-override

Changes the password for MAC authentication.

Syntax

mac-authentication password-override *password*

no mac-authentication password-override *password*

Command Default

The MAC address is the default password for MAC authentication.

Parameters

password

Specifies the password. The password can contain up to 32 alphanumeric characters, but cannot include blank spaces.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the default password (the MAC address).

Examples

The following example changes the password for MAC authentication.

```
device (config)# mac-authentication password-override sub1
```

History

Release version	Command history
08.0.20	This command was replaced on Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750 by the **mac-authentication password-override (Flexible authentication)** command.

mac-authentication password-override (Flexible authentication)

Enables password override for MAC authentication and specifies a user-defined password instead of the MAC address for MAC authentication.

Syntax

mac-authentication password-override *password*

no mac-authentication password-override *password*

Command Default

MAC authentication password override is not enabled.

Parameters

password

Specifies the password to be used for MAC authentication. The password can contain up to 32 alphanumeric characters, but cannot include blank spaces.

Modes

Authentication configuration mode

Usage Guidelines

The **no** form disables MAC authentication password override.

The MAC address is still the user name and cannot be changed.

Examples

The following example enables MAC authentication password override on the device.

```
device(config)# authentication
device(config-authen)# mac-authentication password-override password
```

History

Release version	Command history
08.0.20	This command was introduced.

mac-authentication save-dynamicvlan-to-config

Saves dynamic VLAN assignments to the running-config file.

Syntax

mac-authentication save-dynamicvlan-to-config

no mac-authentication save-dynamicvlan-to-config

Command Default

Dynamic VLAN assignments are not saved to the running-config file.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the configuration to save the dynamic VLAN assignments to the running-config file.

Examples

The following example saves dynamic VLAN assignments to the running-config file.

```
device (config)# mac-authentication save-dynamicvlan-to-config
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac filter

Configures MAC address filters.

Syntax

mac filter *filter-num* { **permit** | **deny** } { *source-mac source-mask* | **any** } { *destination-mac destination-mask* | **any** } [**mirror**]

no mac filter *filter-num* { **permit** | **deny** } { *source-mac source-mask* | **any** } { *destination-mac destination-mask* | **any** } [**mirror**]

Command Default

MAC address filters are not configured.

Parameters

filter-num
: Configures the MAC address filter ID. You can configure up to 507 MAC address filters. The default value is 512.

permit
: Permits the traffic.

deny
: Denies the traffic.

source-mac
: Configures the source Ethernet MAC address.

source-mask
: Specifies the mask using f (ones) and zeros.

any
: Configures the filter to match all source MAC addresses.

destination-mac
: Configures the destination Ethernet MAC address.

destination-mask
: Specifies the mask using f (ones) and zeros.

any
: Configures the filter to match all destination MAC addresses.

mirror
: Mirrors traffic that matches against configured entry.

Modes

Global configuration mode

Usage Guidelines

Once the MAC address filters are configured, you must apply the MAC address filters to a port.

The **no** form of the command removes the MAC address filters.

Examples

The following example shows how to configure and apply MAC address filters. In this example, filter 1 is configured to deny traffic with a source MAC address that begins with "3565" to any destination, and filters 2 through 5 are configured to deny traffic with the specified destination MAC addresses. Filter 1024 permits all traffic that is not denied by any other filter.

```
device(config)# mac filter 1 deny 0000.0075.3676 ffff.0000.0000
device(config)# mac filter 2 deny any ffff.ffff.ffff ffff.ffff.ffff
device(config)# mac filter 3 deny any 0180.c200.0000 ffff.ffff.fff0
device(config)# mac filter 4 deny any 0000.0034.5678 ffff.ffff.ffff
device(config)# mac filter 5 deny any 0000.0045.6789 ffff.ffff.ffff
device(config)# mac filter 1024 permit any any
```

mac filter enable-accounting

Enables access control list (ACL) accounting on Layer 2 MAC filters.

Syntax

mac filter *num* **enable-accounting**

no mac filter *num* **enable-accounting**

Command Default

This option is disabled.

Parameters

num

Specifies the MAC filter ID.

enable-accounting

Enables MAC filter accounting on the specified interface.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables ACL accounting on the associated Layer 2 MAC filter interface.

Examples

The following example enables ACL accounting on a Layer 2 MAC filter.

```
device(config)# mac filter 1 permit 0000.0000.0001 ffff.ffff.ffff any
device(config)# mac filter 1 enable-accounting
device(config)# interface ethernet 3/21
device(config-if-e1000-3/21)# mac filter-group 1
```

History

Release version	Command history
08.0.10	This command was introduced.

mac filter-group

Applies a group of MAC address filters to a port.

Syntax

mac filter-group *filter-num* [[*filter-num* **to** *filter-num* | *filter-num*] ...]

no mac filter-group *filter-num* [[*filter-num* **to** *filter-num* | *filter-num*] ...]

Command Default

MAC address filters are not applied to any port.

Parameters

filter-num

Specifies the MAC address filter ID.

to *filter-num*

Specifies the range of MAC address filter IDs.

Modes

Interface configuration mode

Usage Guidelines

When applying the filter group to the interface, specify each line to be applied separately or use the **to** keyword to apply a consecutive range of filter lines, for example, 1 3 to 8 10.

The filters must be applied as a group. For example, if you want to apply four filters to an interface, they must all appear on the same command line.

You cannot add or remove individual filters in the group. To add or remove a filter on an interface, apply the filter group again containing all the filters you want to apply to the port. If you apply a filter group to a port that already has a filter group applied, the older filter group is replaced by the new filter group.

The **no** form of the command removes the MAC address filters configured on a port.

Examples

The following exmaple configures MAC address filters and applies them to a port.

```
device(config)# mac filter 1 deny 0000.0075.3676 ffff.0000.0000
device(config)# mac filter 2 deny any ffff.ffff.ffff ffff.ffff.ffff
device(config)# mac filter 3 deny any 0180.c200.0000 ffff.ffff.fff0
device(config)# mac filter 4 deny any 0000.0034.5678 ffff.ffff.ffff
device(config)# mac filter 5 deny any 0000.0045.6789 ffff.ffff.ffff
device(config)# mac filter 1024 permit any any
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# mac filter-group 1 to 5 1024
```

mac filter-group log-enable

Enables logging for MAC address filtered packets on a specific port.

Syntax

mac filter-group log-enable

no mac filter-group log-enable

Command Default

Logging for MAC address filtered packets on specific ports is disabled.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables logging for MAC address filtered packets on specific ports.

When a MAC address filter is applied to or removed from an interface, a syslog message is generated.

Examples

The following example enables logging for filtered packets on the Ethernet interface 1/1/1.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# mac filter-group log-enable
```

mac filter log-enable

Globally enables logging for MAC address filtered packets.

Syntax

mac filter log-enable

no mac filter log-enable

Command Default

Logging is disabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables logging of MAC address filtered packets.

Examples

The following example globally enables logging for MAC address filtered packets.

```
device(config)# mac filter log-enable
```

mac-learn-disable

Disables a physical port from automatic learning the source MAC address.

Syntax

mac-learn-disable

no mac-learn-disable

Command Default

By default, when a packet with an unknown source MAC address is received on a port, the Brocade device learns this MAC address on the port.

Modes

Interface configuration mode

Usage Guidelines

This command is not available on virtual routing interfaces. Also, if this command is configured on the primary port of a LAG, MAC address learning (source MAC address) will be disabled on all the ports in the LAG.

Entering the command on a tagged ports disables source MAC address learning for that port in all VLANs of which that port is a member. For example, if tagged port 1/1/1 is a member of VLAN 10, 20, and 30 and you issue the **mac-learn-disable** command on port 1/1/1, port 1/1/1 will not learn source MAC addresses, even if it is a member of VLAN 10, 20, and 30.

The **no** form of the command allows a physical port to learn source MAC addresses.

Examples

The following example disables the automatic learning of the source MAC address.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# mac-learn-disable
```

mac-notification interval

Configures the MAC-notification interval between each set of generated traps.

Syntax

mac-notification interval *secs*

no mac-notification interval *secs*

Command Default

No interval for MAC-notification is configured.

Parameters

secs

Specifies the MAC-notification interval in seconds between each set of traps that are generated. The range is from 1 through 3600 seconds (1 hour). The default interval is 3 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command sets the interval to its default value, which is 3 seconds.

A trap is sent aggregating the MAC events such as addition or deletion depending on the interval you specify.

Examples

The following example configures an interval of 40 seconds.

```
device(config)# mac-notification interval 40
```

The following example sets the interval to its default value:

```
device(config)# no mac-notification interval 3
```

History

Release version	Command history
08.0.10	This command was introduced.

mac-movement notification

Enables movement notifications and collects statistics for the movement of MAC addresses.

Syntax

mac-movement notification { **interval-history** *seconds* | **threshold-rate** *moves* **sampling-interval** *seconds* }

no mac-movement notification { **interval-history** *seconds* | **threshold-rate** *moves* **sampling-interval** *seconds* }

Parameters

interval-history *seconds*
: Configures the time interval during which the MAC address movement notification data is collected and enables a corresponding SNMP trap.

threshold-rate *moves*
: Configures the number of times a MAC address can move within the specified period until an SNMP trap is sent.

sampling-interval *seconds*
: Configures the sampling interval.

Modes

Global configuration mode

Usage Guidelines

The interval history includes statistical information such as the number of MAC addresses that move over the specified period, the total number of MAC address moves, which MAC addresses have moved, and how many times a MAC address has moved.

There is an upper limit on the number of MAC addresses for which MAC address-specific data is collected. This limit is necessary because it is not possible to report on all MAC addresses when many move.

Avoid threshold rates and sampling intervals that are too small. If you choose a small threshold and a sampling interval that is also small, an unnecessary high number of traps could occur.

The **no** form of the command disables movement notifications and stops collecting statistics for the movement of MAC addresses.

Examples

The following example sets the notification interval to 300 seconds.

```
device(config)# mac-movement notification interval-history 300
```

The following example sets the notification for 500 moves and a sampling interval of 400 seconds.

```
device(config)# mac-movement notification threshold-rate 500 sampling-interval 400
```

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** | **gcm-aes-128 integrity-only** }

no macsec cipher-suite { **gcm-aes-128** | **gcm-aes-128 integrity-only** }

Command 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.

gcm-aes-128 integrity-only
Enables GCM-AES-128 bit integrity checks.

Modes

dot1x-mka-cfg-group mode

Usage Guidelines

The **no** form of the command restores the default encryption and integrity checking.

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

The **macsec cipher-suite** command can be used in conjunction with an encryption offset configured with the **macsec confidentiality-offset** command.

Examples

The following example enables GCM-AES-128 encryption on group test1.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128
```

The following example enables GCM-AES-128 bit integrity checking on test1.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128 integrity-only
```

History

Release version	Command history
08.0.20	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

The default value for the MACsec encryption offset size is zero (0).

Parameters

size

Determines where encryption begins. Valid values are:

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

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

The **no** form of the command disables encryption offset on all interfaces in the MACsec MKA group.

This command is only meaningful when encryption is enabled for the MACsec group using the **macsec cipher-suite** command.

Examples

The following example configures a 30-byte offset on encrypted transmissions as part of group test1 parameters.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka)# macsec cipher-suite gcm-aes-128
device(config-dot1x-mka-group-test1)# macsec confidentiality-offset 30
```

History

Release version	Command history
08.0.20	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

MACsec frame validation is disabled (not visible in configuration).

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

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

The **no** form of the restores the default (validation checks for frames with MACsec headers is disabled).

Examples

The following example enables validation checks for frames with MACsec headers on group test1 and configures strict validation mode.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec frame-validation strict
```

History

Release version	Command history
08.0.20	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* } [**disable**]

no macsec replay-protection { **strict** | **out-of-order window-size** *size* } [**disable**]

Command Default

Parameters

strict

Does not allow out-of-order packets.

out-of-order window-size

Allows out-of-order packets within a specific window size.

size

Specifies the allowable window within which an out-of-order packet can be received. Allowable range is from 0 through 4294967295.

disable

Available only for the ICX 7450. Disables replay protection.

Modes

dot1x-mka-cfg-group mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, it is also supported on the ICX 7450.

The **no** form of the command disables macsec replay protection.

Examples

The following example configures group test1 to accept packets in exact sequence only.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec replay-protection strict
device(config-dot1x-mka-group-test1)#
```

The following example configures group test1 to accept out-of-order MACsec frames within a window size of 2000.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# macsec replay-protection out-of-order window-size 2000
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.30	The **disable** option for the **macsec replay-protection** command was introduced.

mac-session-aging max-age

Configures the software aging period for the dot1x-MAC-session of a blocked client after which the associated MAC address is aged out.

Syntax

mac-session-aging max-age *time*

no mac-session-aging max-age *time*

Command Default

The default time is 120 seconds.

Parameters

time

Specifies the software aging period for the dot1x-MAC-session of a blocked client after which the associated MAC address is aged out. Valid values are from 1 through 65535.

Modes

dot1x configuration mode

Usage Guidelines

After the software aging period ends, the blocked client MAC address ages out, and can be authenticated again if the Brocade device receives traffic from the client MAC address.

The **no** form of the command resets the software aging period to the default value (120 seconds).

Examples

The following example configures the software aging period for the dot1x-MAC-session of a blocked client after which the associated MAC address is aged out.

```
device(config)# dot1x-enable
device(config-dot1x)# mac-session-aging max-age 250
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

mac-session-aging no-aging

Disables aging of the permitted or denied dot1x-MAC-sessions.

Syntax

mac-session-aging no-aging [**denied-mac-only** | **permitted-mac-only**]

no mac-session-aging no-aging [**denied-mac-only** | **permitted-mac-only**]

Command Default

The dot1x-MAC-sessions for clients authenticated or denied by a RADIUS server are aged out if no traffic is received from the client MAC address for a certain period of time.

Parameters

denied-mac-only

Disables aging of dot1x-MAC-sessions for non-authenticated clients that are blocked by the Brocade device.

permitted-mac-only

Disables aging of dot1x-MAC-sessions for authenticated clients, as well as for non-authenticated clients whose ports are placed in the restricted VLAN, even if no traffic is received from the client MAC address beyond the normal MAC aging interval.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command enables aging of the permitted or denied dot1x-MAC-sessions.

Examples

The following example disables aging of the denied dot1x-MAC-sessions.

```
device(config)# dot1x-enable
device(config-dot1x)# mac-session-aging no-aging denied-mac-only
```

The following example disables aging of the permitted dot1x-MAC-sessions.

```
device(config)# dot1x-enable
device(config-dot1x)# mac-session-aging no-aging permitted-mac-only
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

management-vlan

Configures a VLAN to be a part of the management VLAN.

Syntax

management-vlan

no management-vlan

Command Default

VLAN configuration mode

Modes

VLAN configuration mode

Usage Guidelines

When this command is used, the out-of-band (OOB) interface port is not disabled. The port remains accessible to management even if in-band interface ports are busy forwarding packets at line rate. No packets are shared between the OOB management port and the in-band port.

The port is treated as an untagged port.

The **management-vlan** command is available only in the FastIron switch image.

Use the **no** form of the command to remove the VLAN from the management VLAN.

Examples

To specify a VLAN and assign it to the management VLAN:

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# management-vlan
```

To remove the VLAN from the management VLAN:

```
device(config-vlan-20)# no management-vlan
```

History

Release version	Command history
8.0.30	This command was introduced.

management-vrf

Configures a VRF as a global management VRF.

Syntax

management-vrf *vrf-name*

no management-vrf *vrf-name*

Command Default

Management VRF is not configured.

Parameters

vrf-name

Specifies the name of a pre-configured VRF.

Modes

Global configuration mode

Usage Guidelines

If the VRF is not preconfigured, command execution fails, and an error message is displayed. If you try to delete a management VRF that was not configured, the system displays an error message.

If a VRF is currently configured as the management VRF, it cannot be deleted or modified. Attempting to do so causes the system to return an error message. If a management VRF is already configured, you must remove the existing management VRF configuration before configuring a new one.

The **no** form of the command removes the management VRF. When the management VRF is deleted, a Syslog message is displayed.

Examples

The following example shows how to configure a management-vrf.

```
device(config)# management-vrf mvrf
```

master

Configures the device as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available.

Syntax

master [**stratum** *number*]

no master [**stratum** *number*]

Command Default

The master clock is disabled by default.

Parameters

stratum *number*

Specifies the NTP stratum number that the system will claim. The number can range from 2 to 15. The default value is 8.

Modes

NTP configuration mode

Usage Guidelines

Local time and time zone has to be configured before configuring the master command.

Use the **master** command with caution. It is very easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple machines in the same network with the master command can cause instability in timekeeping if the machines do not agree on the time.

NOTE
This command is not effective, if the NTP is enabled in client-only mode.

The **no** form of the command disables the master clock function.

Examples

The following example shows how to configure the NTP master clock.

```
device(config)# ntp
device(config-ntp)# master stratum 5
```

master (MRP)

Configures a node as the master node for the metro ring.

Syntax

master

no master

Command Default

A master node is not configured.

Modes

MRP configuration mode

Usage Guidelines

The **no** form of the command returns a master node a normal node.

Any node on a metro ring that does not have a shared interface can be designated as the ring master node. A master node can be the master node of more than one ring. However, if all nodes on the ring have shared interfaces, a node that does not have tunnel ports can be designated as the master node of that ring. If none of the nodes meet these criteria, you must change the priorities of the ring by reconfiguring the ring ID.

Examples

The following example shows how to set a node as a master node.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)# name CustomerA
device(config-vlan-2-mrp-1)# master
device(config-vlan-2-mrp-1)# ring-interface ethernet 1/1/1 ethernet 1/1/2
device(config-vlan-2-mrp-1)# enable
```

master-vlan

Adds the master VLAN to the topology group.

Syntax

master-vlan *vlan-id*

no master-vlan *vlan-id*

Command Default

A master VLAN is not configured.

Parameters

vlan-id

Specifies the VLAN ID of the master VLAN.

Modes

Topology group configuration mode

Usage Guidelines

To configure a master VLAN, the VLAN must already be configured. Make sure all the Layer 2 protocol settings in the VLAN are correct for your configuration before you add the VLAN to the topology group. A topology group can have only one master VLAN. If you add a new master VLAN to a topology group that already has a master VLAN, the new master VLAN replaces the older master VLAN. All member VLANs and VLAN groups follow the Layer 2 protocol settings of the new master VLAN.

If you remove the master VLAN (by entering the **no master-vlan** command), the software selects the new master VLAN from member VLANs. A new candidate master VLAN is configured as a member VLAN so that the first added member VLAN will be a new candidate master VLAN. Once you save and reload, a member VLAN with the youngest VLAN ID will be the new candidate master. The new master VLAN inherits the Layer 2 protocol settings of the older master VLAN.

When removing the master VLAN from the topology group, Spanning Tree Protocol (STP) must be disabled on the master VLAN.

The **no** form of the command removes the master VLAN from the topology group.

Examples

The following example adds the master VLAN 2 to the topology group 2.

```
device(config)# topology-group 2
device(config-topo-group-2)# master-vlan 2
```

master-vlan (STP)

Adds the master VLAN to the STP group.

Syntax

master-vlan *vlan-id*

no master-vlan *vlan-id*

Command Default

The master VLAN is not configured.

Parameters

vlan-id

Specifies the VLAN ID of the master VLAN.

Modes

STP group configuration mode

Usage Guidelines

To configure a master VLAN, the VLAN must already be configured. The master VLAN contains the STP settings for all the VLANs in the STP per VLAN group. An STP group can have only one master VLAN. If you add a new master VLAN to an STP group that already has a master VLAN, the new master VLAN replaces the older master VLAN.

If you remove the master VLAN (by entering the **no master-vlan** command), the software selects the new master VLAN from member VLANs. A new candidate master VLAN will be in configured as a member VLAN so that the first added member VLAN will be a new candidate master VLAN. Once you save and reload, a member VLAN with the youngest VLAN ID will be the new candidate master.

The **no** form of the command removes the master VLAN from the STP group.

Examples

The following example adds the master VLAN 2 to the STP group 2.

```
device(config)# stp-group 2
device(config-stp-group-2)# master-vlan 2
```

match as-path

Matches a BGP autonomous system path (AS-path) ACL in a route map instance.

Syntax

match as-path *aspath-name ...*

no match as-path *aspath-name*

Command Default

By default, match statements are not configured.

Parameters

aspath-name

Specifies an AS-path access list.

Modes

Route-map configuration mode

Usage Guidelines

You can specify up to five AS-path ACLs.

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

Examples

The following example configures a route map that matches based on AS-path “myas-path”.

```
device# configure termnial
device(config)# route-map myroutemap permit 1
device(config-routemap myroutemap)# match as-path myas-path
```

match community

Matches a BGP community access list name in a route-map instance.

Syntax

match community *name* [**name ...**] [**exact-match**]

no match community *name* [**name ...**] [**exact-match**]

Command Default

By default, match statements are not configured.

Parameters

name

Specifies a BGP community access list name.

exact-match

Specifies that an exact match is required.

Modes

Route-map configuration mode

Usage Guidelines

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

Examples

The following example configures a route map that matches BGP community access list name “abccommunity”.

```
device# configure termnial
device(config)# route-map myroutemap permit 1
device(config-routemap myroutemap)# match community abccommunity
```

match interface

Configures the interface match clause in a route-map instance.

Syntax

match interface { **ethernet** *stackid /slot/port* | **loopback** *num* | **null0** | **tunnel** *number* | **ve** *vlan-id* } **...**

no match interface { **ethernet** *stackid /slot/port* | **loopback** *num* | **null0** | **tunnel** *number* | **ve** *vlan-id* } **...**

Parameters

ethernet *stackid slot port*
: Specifies an Ethernet interface with stackid, slot,and port numbers.

loopback *num*
: Specifies a loopback interface.

null0
: Specifies a loopback interface.

tunnel *num*
: Specifies a tunnel.

ve *vlan-id*
: Specifies a virtual Ethernet interface.

Modes

Route-map configuration mode

Usage Guidelines

A maximum of five interfaces is supported. There is no restriction on the number or type of each interface specified, as long as the total is less than or equal to five. The **no** form of the command removes the configuration.

Examples

The following example configures a route map based on matching Ethernet interfaces 1/1/3 to 1/1/7.

```
device configure terminal
device(config)# route-map myroutemap permit 10
device(config-routemap myroutemap)# match interface ethernet 1/1/3 ethernet 1/1/7
```

match ip address

Matches IP address conditions in a route map instance.

Syntax

match ip address { *acl-name* | *acl-num* }

no match ip address { *acl-name* | *acl-num* }

Command Default

By default, match statements are not configured.

Parameters

acl-name

Specifies the ACL name.

acl-num

Specifies the ACL number.

Modes

Route map configuration mode

Usage Guidelines

When a route map is used in the PBR, the PBR policy uses up to five ACLs in a matching policy of each route map instance.

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

Examples

The following example configures a PBR route map that matches based on the ACLs and sets routing information in the IP traffic

```
device(config)# route-map test-route permit 99
device(config-routemap test-route)# match ip address 99
device(config-routemap test-route)# set ip next-hop 192.168.2.1
```

match ipv6 address

Matches IPv6 address conditions in a route map instance.

Syntax

match ipv6 address { **prefix-list** *prefix-list-name* }

no match ipv6 address

Command Default

No routes are distributed based on destination network number.

Parameters

prefix-list *prefix-list-name*

Specifies the name of an IPv6 prefix list.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to remove the **match ipv6 address** entry.

Examples

This example matches IPv6 routes that have addresses specified by the prefix list named “myprefixlist”.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap)# match ipv6 address prefix-list myprefixlist
```

match metric

Matches a route metric in a route-map instance.

Syntax

match metric *value*

no match metric *value*

Command Default

By default, match statements are not configured.

Parameters

value

Matches a route metric for the route-map instance.

Modes

Route-map configuration mode

Usage Guidelines

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

Examples

The following example configures a metric that matches on the specified value.

```
device# configure terminal
device(config)# route-map test-route permit 99
device(config-routemap test-route)# match metric 1000
```

match protocol

Matches the routes on protocol types and subtypes in a route-map instance.

Syntax

match interface { **bgp** [**external** | **internal** | **static-network**] | **rip** | **static** }

no match interface { **bgp** [**external** | **internal** | **static-network**] | **rip** | **static** }

Parameters

bgp
Matches BGP routes.

external
Matches eBGP routes.

internal
Matches iBGP routes.

static-network
Matches BGP static routes.

rip
Matches RIP routes.

static
Matches static routes.

Modes

Route-map configuration mode

Usage Guidelines

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

Examples

The following example configures the RIP protocol as a matching criterion for a route-map instance.

```
device configure terminal
device(config)# route-map myroutemap permit 10
device(config-routemap myroutemap)# match protocol rip
```

match route-type

Configures the route type clause in a route-map instance.

Syntax

match route-type { **external-type1** | **external-type2** | **internal** }

no match route-type { **external-type1** | **external-type2** | **internal** }

Parameters

internal

Specifies OSPF internal intra or inter type routes.

external-type1

Specifies OSPF external type 1 routes.

external-type2

Specifies OSPF external type 2 routes.

Modes

Route-map configuration mode

Usage Guidelines

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

Examples

The following example configures OSPF external type 1 routes as a matching criterion for a route-map instance.

```
device# configure terminal
device(config)# route-map myroutemap permit 10
device(config-routemap myroutemap)# match route-type external-type1
```

match tag

Matches a route tag in a route-map instance.

Syntax

match tag *value*

no match tag *value*

Parameters

value

Specifies a route tag and route tag value. Valid values range from 0 through 4294967294.

Modes

Route-map configuration mode

Usage Guidelines

A maximum of 8 tags can be configured.

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

Examples

The following example specifies a route tag value of 6 as a matching criterion for a route-map instance.

```
device# configure terminal
device(config)# route-map myroutemap permit 10
device(config-routemap myroutemap)# match tag 6
```

maximum (Port Security)

Configures the maximum number of secure MAC addresses an interface can store when MAC port security is enabled.

Syntax

maximum *max-num*

no maximum *max-num*

Command Default

By default, when MAC port security is enabled, an interface can store one secure MAC address.

Parameters

max-num

The maximum number of secure MAC addresses that can be configured. The range is from 0 through 64, plus the total number of global resources available. The default is 1.

Modes

Port security configuration mode

Port security interface configuration mode

Usage Guidelines

Besides the maximum of 64 local resources available to an interface, there are additional global resources. Depending on flash memory size, a device can have 1024, 2048, or 4096 global resources available. When an interface has secured enough MAC addresses to reach its limit for local resources, it can secure additional MAC addresses by using global resources. Global resources are shared among all the interfaces on a first-come, first-served basis.

The **no** form of the command sets the maximum number of secure MAC addresses an interface can store to one.

Examples

The following example configures the maximum number of secure MAC addresses an interface can store as 50.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# port security
device(config-port-security-e1000-1/1/1)# maximum 50
```

maximum-paths

Changes the maximum number of BGP4 and BGP4+ shared paths.

Syntax

maximum-paths *num* | **use-load-sharing**

no maximum-paths

Command Default

This option is disabled.

Parameters

num

Maximum number of paths across which the device balances traffic to a given BGP4 destination. Range is from 2 through 8. The default is 1.

use-load-sharing

Uses the maximum IP ECMP path value that is configured by means of the **ip load-sharing** command.

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

Usage Guidelines

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

Use this command to change the maximum number of BGP4 shared paths, either by setting a value or using the value configured by the **ip load-sharing** command.

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.

Examples

This example sets the maximum number of BGP4 shared paths to 8.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# maximum-paths 8
```

This example sets the maximum number of BGP4+ shared paths to that of the value already configured using the **ip load-sharing** command.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths use-load-sharing
```

This example sets the maximum number of BGP4 shared paths to 2 in a nondefault VRF instance in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# maximum-paths 2
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

maximum-paths ebgp ibgp

Specifies the number of equal-cost multipath EBGP or IBGP routes or paths that are selected.

Syntax

maximum-paths { **ebgp** *num* | **ibgp** *num* }

no maximum-paths

Command Default

This option is disabled.

Parameters

ebgp

Specifies EBGP routes or paths.

ibgp

Specifies IBGP routes or paths.

num

The number of equal-cost multipath routes or paths that are selected. Range is from 1 through 8. 1 disables equal-cost multipath.

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

Usage Guidelines

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

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.

Enhancements to BGP4 load sharing support the load sharing of BGP4 and BGP4+ routes in IP Equal-Cost Multipath (ECMP), even if the BGP4 multipath load-sharing feature is not enabled by means of the **use-load-sharing** option to the **maximum-paths** command. You can set separate values for IGMP and ECMP load sharing. Use this command to specify the number of equal-cost multipath EBGP or IBGP routes or paths that are selected.

Examples

This example sets the number of equal-cost multipath EBGP routes or paths that will be selected to 6 in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)#  maximum-paths ebgp 6
```

This example sets the number of equal-cost multipath IBGP routes or paths that will be selected to 4 in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths ibgp 4
```

This example sets the number of equal-cost multipath EBGP routes or paths that will be selected to 3 in a nondefault VRF instance in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# maximum-paths ebgp 3
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

maximum-preference

Configures the Router Advertisement (RA) guard policy to accept RAs based on a router preference setting.

Syntax

maximum-preference { **high** | **low** | **medium** }

no maximum-preference { **high** | **low** | **medium** }

Command Default

The router preference setting for the RA guard policy is high (allows all RAs).

Parameters

high

Configures the router preference of RAs for the RA guard policy to high (allows all RAs). This is the default.

low

Allows RAs of low router preference.

medium

Allows RAs of low and medium router preference.

Modes

RA guard policy configuration mode

Usage Guidelines

If a very low value is set, the RAs expected to be forwarded might get dropped.

The **no** form of this command removes the router preference for an RA guard policy.

Examples

The following example configures the RA guard policy router preference to low:

```
Brocade(config)# ipv6 raguard policy p1
Brocade(config-ipv6-RAG-policy p1)# maximum-preference low
```

maxreq

Configures the maximum number of Extensible Authentication Protocol (EAP) request/identity frame retransmissions.

Syntax

maxreq *count*

no maxreq *count*

Command Default

The device retransmits the EAP request/identity frame a maximum of two times.

Parameters

count

Specifies the maximum number of times the device retransmits the EAP request/identity frame. The value range is from 1 through 10.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command resets the maximum number of EAP request/identity frame retransmissions to the default value (2).

Examples

The following example configures the device to retransmit the EAP request/identity frame to a client a maximum of three times.

```
device(config)# dot1x-enable
device(config-dot1x)# maxreq 3
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

max-hw-age

Enables and configures the maximum hardware age for denied MAC addresses.

Syntax

max-hw-age *age*

no max-hw-age *age*

Command Default

The maximum hardware age is not configured. The default hardware aging time is 70 seconds.

Parameters

age

Specifies the maximum hardware age in seconds. The possible values range from 1 to 65535 seconds.

Modes

Authentication mode

Usage Guidelines

The **no** form of this command disables maximum hardware age.

MAC addresses that are authenticated or denied by a RADIUS server are aged out if no traffic is received from the MAC address for a certain period of time (hardware aging period + software aging period).

Examples

The following example enables maximum hardware age and sets it to 160 seconds.

```
device(config)# authentication
device(config-authen)# max-hw-age 160
```

History

Release version	Command history
08.0.20	This command was introduced.

max-mcache

Configures the maximum number of PIM cache entries.

Syntax

max-mcache *num*

no max-mcache *num*

Command Default

If this command is not configured, the maximum value is determined by the **system max pim-hw-mcache** command or by available system resources.

Parameters

num

Specifies the maximum number of multicast cache entries for PIM.

Modes

PIM router configuration mode

PIM router VRF mode

Usage Guidelines

The **no** form of this command removes the configuration and resets the command to its default behavior.

Configure the **max-mcache** command to define the maximum number of repeated cache entries for PIM traffic being sent from the same source address and being received by the same destination address. To define this maximum for the default VRF, configure the command in router PIM configuration mode; to define the maximum for a specific VRF, first configure the **router pim vrf** command.

Examples

This example configures the maximum number of PIM cache entries for the default VRF to 999.

```
device(config)# router pim
device(config-pim-router)# max-mcache 999
```

This example configures the maximum number of PIM cache entries for the VRF, VPN1, to 999.

```
device(config)# router pim vrf vpn1
device(config-pim-router-vrf-vpn1)# max-mcache 999
```

max-sw-age

Configures the maximum software age for denied MAC addresses.

Syntax

max-sw-age *age*

no max-sw *age*

Command Default

The maximum software age is not configured.

Parameters

age

You can specify from 1 - 65535 seconds. The default is 120 seconds.

Modes

Authentication mode

Usage Guidelines

After normal MAC aging period for permitted clients (or clients in restricted VLAN) or hardware aging period for blocked clients, the software aging period begins. After the software aging period ends, the client session ages out and can be authenticated again if the Brocade device receives traffic from the MAC address.

Examples

The following example configures the maximum software age to 170 seconds.

```
device(config)# authentication
device(config-authen)# max-sw-age 170
```

History

Release version	Command history
08.0.20	This command was introduced.

med-missing-as-worst

Configures the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

Syntax

med-missing-as-worst

no med-missing-as-worst

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-router)# med-missing-as-worst
```

member-group

Adds the member VLAN group to the topology group.

Syntax

member-group *number*

no member-group *number*

Command Default

A member VLAN group is not added to the topology group.

Parameters

number

Specifies the member VLAN group ID.

Modes

Topology group configuration mode

Usage Guidelines

The **no** form of the command removes the member VLAN group.

The VLAN group must already be configured.

Once you add a VLAN group as a member of a topology group, all the Layer 2 protocol configuration information for the VLAN group is deleted. For example, if STP is configured on a VLAN and you add the VLAN to a topology group, the STP configuration is removed from the VLAN. Once you add the VLAN to a topology group, the VLAN uses the Layer 2 protocol settings of the master VLAN. If you remove a member VLAN group from a topology group, you must reconfigure the Layer 2 protocol information in the VLAN group.

Examples

The following example shows how to add a member VLAN group:

```
device(config)# topology-group 2
device(config-topo-group-2)# member-group 2
```

member-group (STP)

Adds the member VLAN group to the STP group.

Syntax

member-group *number*

no member-group *number*

Command Default

A member VLAN group is not added to the STP group.

Parameters

number

Specifies the member VLAN group ID.

Modes

STP group configuration mode

Usage Guidelines

The VLAN group must already be configured. All the VLANs in the member group inherit the STP settings of the master VLAN in the group.

The **no** form of the command removes the member VLAN group.

Examples

The following example shows how to add a member VLAN group.

```
device(config)# stp-group 2
device(config-stp-group-2)# member-group 2
```

member-vlan

Adds members to the VLAN topology group.

Syntax

member-vlan *vlan-id* [**to** *vlan-id* | [*vlan-id* **to** *vlan-id* | *vlan-id*]...]

no member-vlan *vlan-id* [**to** *vlan-id* | [*vlan-id* **to** *vlan-id* | *vlan-id*]...]

Command Default

Member VLANs are not added to the VLAN topology group.

Parameters

vlan-id

Adds a member VLAN ID to the topology group.

to *vlan-id*

Adds the range of member VLANs to the topology group.

Modes

Topology group configuration mode

Usage Guidelines

The member VLAN group must configured before adding it to the topology group.

Each topology group can control up to 4096 VLANs. The VLANs within a VLAN group have the same ports and use the same values for other VLAN parameters.

Once you add a VLAN as a member of a topology group, all the Layer 2 protocol configuration information for the VLAN is deleted. For example, if STP is configured on a VLAN and you add the VLAN to a topology group, the STP configuration is removed from the VLAN. Once you add the VLAN to a topology group, the VLAN uses the Layer 2 protocol settings of the master VLAN. If you remove a member VLAN from a topology group, you must reconfigure the Layer 2 protocol information in the VLAN or VLAN group.

The **no** form of the command removes the member VLANs from the topology group.

Examples

The following example adds the members to the VLAN topology group.

```
device(config)# topology-group 2
device(config-topo-group-2)# member-vlan 4
device(config-topo-group-2)# member-vlan 5
```

member-vlan (STP)

Adds member VLANs to the STP group.

Syntax

member-vlan *vlan-id* [**to** *vlan-id* | [*vlan-id* **to** *vlan-id* | *vlan-id*]...]

no member-vlan *vlan-id* [**to** *vlan-id* | [*vlan-id* **to** *vlan-id* | *vlan-id*]...]

Command Default

Member VLANs are not added to the STP group.

Parameters

vlan-id

Adds a member VLAN ID to the STP group.

to *vlan-id*

Adds the range of member VLANs to the STP group.

Modes

STP group configuration mode

Usage Guidelines

The member VLAN group must be configured before adding it to the STP group.

All the VLANs in the member group inherit the STP settings of the master VLAN in the group.

The **no** form of the command removes the member VLANs from the STP group.

Examples

The following example adds the member VLANs to the STP group.

```
device(config)# stp-group 2
device(config-stp-group-2)# member-vlan 4
device(config-stp-group-2)# member-vlan 5
```

mesh-group

Configures a multicast source discovery protocol (MSDP) mesh group from several rendezvous points (RPs).

Syntax

mesh-group *group-name peer-address*

no mesh-group *group-name peer-address*

Command Default

Mesh groups are not configured.

Parameters

group-name

Specifies the mesh group as alphabetic characters. The limit is 31 characters.

peer-address

Specifies the IP address of the MSDP peer that is being placed in the mesh group. Each mesh group can include up to 32 peers.

Modes

MSDP VRF configuration mode

Usage Guidelines

The **no** form of this command removes mesh groups.

You must configure the **msdp-peer** command to configure the MSDP peers by assigning their IP addresses and the loopback interfaces before you configure a mesh group.

You can have up to four mesh groups in a multicast network. Each mesh group can include up to 15 peers.

Each device that will be part of a mesh group must have a mesh group definition for all the peers in the mesh-group.

Examples

This example configures an MSDP mesh group on each device that will be included in the mesh group.

```
Device(config)# router msdp
Device(config-msdp-router)# msdp-peer 206.251.18.31 connect-source loopback 2
Device(config-msdp-router)# msdp-peer 206.251.19.31 connect-source loopback 2
Device(config-msdp-router)# msdp-peer 206.251.20.31 connect-source loopback 2
Device(config-msdp-router)# mesh-group GroupA 206.251.18.31
Device(config-msdp-router)# mesh-group GroupA 206.251.19.31
Device(config-msdp-router)# mesh-group GroupA 206.251.20.31
Device(config-msdp-router)# exit
```

message-interval

Changes the default PIM Sparse join or prune message interval.

Syntax

message-interval [**vrf** *vrf-name*] *interval*

no message-interval [**vrf** *vrf-name*] *interval*

Parameters

vrf *vrf-name*
: Specifies a VRF instance.

interval
: Specifies the join or prune message interval in seconds. The range is 10 through 18724; the default is 60.

Command Default

The join or prune interval is 60 seconds.

Modes

PIM router configuration mode

PIM router VRF configuration mode

Usage Guidelines

The **no** form of this command restores the default; the join-prune interval is 60 seconds.

PIM Sparse join and prune messages inform other PIM Sparse routers about clients who want to become receivers (join) or stop being receivers (prune) for PIM Sparse groups.

NOTE
Configure the same join or prune message interval on all the PIM Sparse routers in the PIM Sparse domain. The performance of PIM Sparse can be adversely affected if the routers use different timer intervals.

Examples

This example changes the PIM join or prune interval to 30 seconds.

```
Device(config)# ipv6 router pim
Device(config-ipv6-pim-router)# message-interval 30
```

This example changes the PIM join or prune interval on a VRF to 30 seconds.

```
Device(config)# ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)# message-interval 30
```

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
```

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 1023. 256 is reserved for VSRP.

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)#
```

metro-rings

Adds more than one metro rings to a port-based VLAN.

Syntax

metro-rings *ring-id* [*ring-id*...]

no metro-rings *ring-id* [*ring-id*...]

Command Default

Metro rings are not added to a port-based VLAN.

Parameters

ring-id

Specifies the metro ring IDs to be added on a port-based VLAN. The range is from 1 through 1023. 256 is reserved for VSRP.

Modes

VLAN configuration mode

Usage Guidelines

On FCX and ICX devices, use **metro-rings** in addition to the **metro-ring** command. Because these devices do not support MAC address filtering, the **metro-rings** command greatly reduces the number of forward database (FDB) entries.

The **no** form of the command removes the metro rings from the port-based VLAN.

Examples

The following example adds metro rings.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 3
device(config-vlan-2)# metro-rings 1 2
```

mdi-mdix

Enables or disables Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDIX) detection on all Gbps Ethernet Copper ports.

Syntax

mdi-mdix { **mdi** | **mdix** | **auto** }

no mdi-mdix [**mdi** | **mdix** | **auto**]

Command Default

The auto MDI/MDIX detection feature is enabled on all Gbps copper ports.

Parameters

mdi

Turns off automatic MDI/MDIX detection and defines a port as an MDI only port.

mdix

Turns off automatic MDI/MDIX detection and defines a port as an MDIX only port.

auto

Enables automatic detection MDI/MDIX detection on a port.

Modes

Interface configuration mode

Usage Guidelines

The auto MDI/MDIX detection feature can automatically correct errors in cable selection, making the distinction between a straight-through cable and a crossover cable insignificant. The command applies to copper ports only.

NOTE
The **mdi-mdix mdi** and **mdi-mdix mdix** commands work independently of auto-negotiation. Thus, these commands work whether auto-negotiation is turned ON or OFF.

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

Examples

The following example shows how turn off automatic MDI/MDIX detection and define a port as an MDI only port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# mdi-mdix mdi
```

The following example shows how turn on automatic MDI/MDIX detection on a port that was previously set as an MDI or MDIX port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# mdi-mdix auto
```

mirror-port

Configures port mirroring on individual ports.

Syntax

mirror-port ethernet *stackid/slot/port* [**input** | **output**]

no mirror-port ethernet *stackid/slot/port* [**input** | **output**]

Command Default

Ports are not mirrored.

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet port to which mirrored traffic is copied.

input

Copies the ingress traffic.

output

Copies the egress traffic.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure ports to which the monitored traffic is copied. If you do not specify the traffic type, both types of traffic apply. The input and output mirroring ports can be on different ports.

All FastIron devices can have one mirroring port that monitors multiple ports, but cannot have multiple mirror ports for one monitored port. If the mirror port and the monitored ports are on different stack units, only one active mirror port is allowed for the entire traditional stack. If the mirror port and the monitored ports are on the same port region, multiple active mirror ports are allowed for the entire traditional stack. Devices in a traditional stack support 24 ports per port region.

NOTE
Port-based mirroring and VLAN-based mirroring cannot be enabled on a port at the same time.

The **no** form of the command removes the mirrored ports.

Examples

The following example shows the port mirroring configuration.

```
device(config)# mirror-port ethernet 1/2/4
```

mka-cfg-group

Creates and names a MACsec Key Agreement (MKA) configuration group.

Syntax

mka-cfg-group *group-name*

no mka-cfg-group *group-name*

Command Default

No MACsec options are configured for an MKA configuration group. All related parameters retain their default settings.

Parameters

group-name

Provides a name for an MKA configuration group that can be applied to ports.

Modes

dot1x-mka configuration mode

dot1x-mka-interface configuration mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

The **no** form of this command deletes the MKA configuration group. MACSec is disabled on the ports where the group is configured.

The **dot1x-mka-enable** command must be executed before the **mka-cfg-group** command can be used.

After the MACsec Key Agreement (MKA) configuration group is created, you can apply the configured group and its settings to an interface being configured using the **mka-cfg-group** command in the dot1x-mka-interface configuration mode.

Examples

The following example creates the MKA configuration group test1.

```
device(config)# dot1x-mka
  dot1x-mka-enable              Enable MACsec
device(config)# dot1x-mka-enable
device(config-dot1x-mka)#
device(config-dot1x-mka)# mka-cfg-group
  ASCII string   Name for this group
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# key-server-priority
  DECIMAL   Priority of the Key Server. Valid values should be between 0 and 255
device(config-dot1x-mka-group-test1)# key-server-priority 5
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec cipher-suite
  gcm-aes-128   GCM-AES-128 Cipher suite
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec confidentiality-offset
  30   Confidentiality offset of 30
  50   Confidentiality offset of 50
device(config-dot1x-mka-group-test1)# macsec confidentiality-offset 30
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec frame-validation
  check     Validate frames with secTAG and accept frames without secTAG
  disable   Disable frame validation
  strict    Validate frames with secTAG and discard frames without secTAG
device(config-dot1x-mka-group-test1)# macsec frame-validation strict
device(config-dot1x-mka-group-test1)#

device(config-dot1x-mka-group-test1)# macsec replay-protection
  out-of-order   Validate MACsec frames arrive in the given window size
  strict         Validate MACsec frames arrive in a sequence
device(config-dot1x-mka-group-test1)# macsec replay-protection strict
device(config-dot1x-mka-group-test1)#
```

The following example applies the previously configured MKA group test1 to ethernet interface 1/3/3.

```
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# enable-mka ethernet 1/3/3
device(config-dot1x-mka-1/3/3)# mka-cfg-group test1
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20a	This command was expanded to support the association of a configured MKA group and its settings to an interface at the interface configuration level. The **mka-group** command was deprecated as part of this change.

monitor (LAG)

Monitors an individual port in a deployed LAG.

Syntax

monitor { **ethe-port-monitored** *stackid/slot/port* | **named-port-monitored** *name* } [**ethernet** *stackid/slot/port*] { **input** | **output** | **both** }

no monitor{ **ethe-port-monitored** *stackid/slot/port* | **named-port-monitored** *name* } [**ethernet** *stackid/slot/port*] { **input** | **output** | **both** }

Command Default

Traffic is not monitored on ports.

Parameters

ethe-port-monitored *stackid/slot/port*
Specifies the Ethernet port to be monitored.

named-port-monitored *name*
Specifies the named port that you want to monitor.

ethernet *stackid/slot/port*
Specifies the mirror ports to be used and specifies the port to which the traffic analyzer is attached.

input
Monitors the incoming packets.

output
Monitors the outgoing packets.

both
Monitors both incoming and outgoing packets.

Modes

LAG configuration mode

Usage Guidelines

By default, when you monitor the primary port in a LAG group, aggregated traffic for all the ports in the LAG is copied to the mirror port.

You can configure the device to monitor individual ports in a LAG including Ethernet ports or named ports. You can monitor the primary port or another member port individually. Once a LAG is deployed and a primary port is specified using the **primary-port** command, monitoring across all ports of the LAG can be configured at the primary port. If a new port is added to a deployed LAG and if the entire LAG is monitored, the new port will also be mirrored by the same port monitoring traffic across the entire LAG.

NOTE
You can use only one mirror port for each monitored LAG port. You cannot configure mirroring on an undeployed LAG.

The **no** form of the command stops monitoring the traffic.

Examples

The following is an example of monitoring traffic on an individual Ethernet port within a LAG.

```
device(config)# lag test2 dynamic
device(config-lag-test2)# ports ethernet 1/1/1 ethernet 1/1/9
device(config-lag-blue)# primary-port 1/1/1
device(config-lag-blue)# deploy
device(config-lag-test2)# monitor ethe-port-monitored 1/1/1 ethernet 1/1/9 input
```

The following example shows the monitoring of traffic on a named port.

```
device(config)# lag test2 dynamic
device(config-lag-test2)# ports ethernet 1/1/1 ethernet 1/1/9
device(config-lag-test2)# monitor named-port-monitored port1 both
```

monitor

Configures monitoring of the mirrored ports.

Syntax

monitor [**ethernet** *stackid/slot/port*] { **both** | **input** | **output** }

no monitor [**ethernet** *stackid/slot/port*] { **both** | **input** | **output** }

Command Default

Ports are not monitored.

Parameters

ethernet *stackid/slot/port*
: Specifies the mirror port to be used.

both
: Monitors both incoming and outgoing traffic on the mirrored port.

input
: Monitors the ingress traffic on the mirrored port.

output
: Monitors the egress traffic on the mirrored port.

Modes

Interface configuration mode

VLAN configuration mode

Usage Guidelines

If you configure both ACL mirroring and ACL-based rate limiting on the same port, then all packets that match are mirrored, including the packets that exceed the rate limit. The same port cannot be both a monitored port and the mirror port. The same port can be monitored by one mirror port for ingress traffic and another mirror port for egress traffic. The mirror port cannot be a LAG port. More than one monitored port can be assigned to the same mirror port.

For stacked devices, if the ingress and egress analyzer ports are always network ports on the local device, each device may configure the ingress and egress analyzer port independently. However, if you need to mirror to a remote port, then only one ingress and one egress analyzer port are supported for the entire system.

The **no** form of the command stops monitoring the mirrored ports.

Examples

The following example shows how to monitor the mirrored ports.

```
device(config)# interface ethernet 1/2/11
device(config-if-e1000-1/2/11)# monitor ethernet 1/2/4 both
```

The following example shows how to configure VLAN-based mirroring.

```
device(config)# mirror-port ethernet 1/1/21 input
device(config)# vlan 10
device(config-vlan-10)# monitor ethernet 1/1/21
device(config-vlan-10)# exit
device(config)# vlan 20
device(config-vlan-20)# monitor ethernet 1/1/21
device(config-vlan-20)# end
```

mount disk0

Mounts the filesystem of the external USB.

Syntax

mount disk0

Modes

User EXEC mode.

Examples

This example mounts the filesystem of the external USB.

```
device# mount disk0
```

History

Release version	Command history
08.0.30	This command was introduced.

mstp admin-edge-port

Configures ports as operational edge ports.

Syntax

mstp admin-edge-port ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no mstp admin-edge-port ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

Ports are not configured as edge ports.

Parameters

ethernet *stackid/slot/port*

Configures the specified Ethernet port as the edge port.

to *stackid/slot/port*

Configures the specified range of Ethernet ports as edge ports.

Modes

Global configuration mode

Usage Guidelines

You can define specific ports as edge ports for the region in which they are configured to connect to devices (such as a host) that are not running STP, RSTP, or MSTP. If a port is connected to an end device such as a PC, the port can be configured as an edge port.

The **no** form of the command removes a port from being an edge port.

Examples

The following example shows how to configure an Ethernet port as an edge port.

```
device(config)# mstp admin-edge-port ethernet 1/3/1
```

mstp admin-pt2pt-mac

Creates a point-to-point link between ports to increase the speed of convergence.

Syntax

mstp admin-pt2pt-mac ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no mstp admin-pt2pt-mac ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

By default, a point-to-point link is not available between ports.

Parameters

ethernet *stackid/slot/port*

Configures the specified Ethernet port to be a point-to-point link.

to *stackid/slot/port*

Configures the range of specified Ethernet ports to be point-to-point link.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the point-to-point link on the ports.

Examples

The following example shows how to create point-to-point link.

```
device(config)# mstp admin-pt2pt-mac ethernet 1/2/5 ethernet 1/4/5
```

mstp disable

Disables MSTP on Ethernet interfaces.

Syntax

mstp disable ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no mstp disable ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

MSTP is not enabled by default.

Parameters

ethernet *stackid/slot/port*
Disables MSTP on the specified Ethernet interface.

to *stackid/slot/port*
Disables MSTP on a range of Ethernet interfaces.

Modes

Global configuration mode

Usage Guidelines

When a port is disabled for MSTP, the port blocks all the VLAN traffic that is controlled by Multiple Spanning Tree Protocol (MSTP) instance and the Common and Internal Spanning Tree (CIST) instances.

The **no** form of the command enables MSTP.

Examples

The following example shows how to disable MSTP.

```
device(config)# mstp disable ethernet 1/2/1
```

mstp edge-port-auto-detect

Automatically sets a port as an operational edge port.

Syntax

mstp edge-port-auto-detect

no mstp edge-port-auto-detect

Command Default

Ports are not automatically set as edge ports.

Modes

Global configuration mode

Usage Guidelines

You can configure a Layer 3 switch to automatically set a port as an operational edge port if the port does not receive any BPDUs from the time of link-up. If the port receives a BPDU later, the port is automatically reset to become an operational non-edge port.

NOTE
After configuring, it takes the port about three seconds longer to come to the enable state.

The **no** form of the command resets the port as a non-operational edge port.

Examples

The following example shows how to automatically set ports as edge ports.

```
device(config)# mstp edge-port-auto-detect
```

mstp force-migration-check

Triggers a port to force transmit an MSTP BPDU.

Syntax

mstp force-migration-check ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no mstp force-migration-check ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

Ports are not configured to force transmit MSTP BPDUs.

Parameters

ethernet *stackid/slot/port*

Configures the specified Ethernet port to force tranmist an MSTP BPDU.

to *stackid/slot/port*

Configures the specified range of the Ethernet interfaces to force transmit MSTP BPDUs.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the force transmit of an MSTP BPDU.

Examples

The following example triggers the port to transmit an MSTP BPDU.

```
device(config)# mstp force-migration-check ethernet 1/3/1
```

mstp force-version

Configures the bridge to send BPDUs in a specific format.

Syntax

mstp force-version *mode*

no mstp force-version *mode*

Command Default

By default, the bridge sends the BPDUs in MSTP mode (3).

Parameters

mode

Forces the bridge to send BPDUs in a specific format: 0 for STP compatibility mode, 2 for RSTP compatibility mode, and 3 for MSTP mode.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the mode to MSTP mode.

Examples

The following example configures the bridge to forward BPDUs in STP compatibility mode.

```
device(config)# mstp force-version 0
```

mstp forward-delay

Configures the length of time a port waits before it forwards an RST BPDU after a topology change.

Syntax

mstp forward-delay *time*

no mstp forward-delay *time*

Command Default

The default is 15 seconds.

Parameters

time

Configures the time period a port waits before it forwards an RST BPDU after a topology change. The period ranges from 4 through 30 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the value to the default value of 15 seconds.

Examples

The following example configures the time period the port waits before it forwards an RST BPDU after a topology change to 10 seconds.

```
device(config)# mstp forward-delay 10
```

mstp hello-time

Configures the interval between two Hello packets.

Syntax

mstp hello-time *time*

no mstp hello-time *time*

Command Default

By default, the interval is 2 seconds.

Parameters

time

The time interval between two Hello packets. The value ranges from 1 through 10 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the interval to the default (2 seconds).

Examples

The following example configures the interval between two Hello packets to 5 seconds.

```
device(config)# mstp hello-time 5
```

mstp instance

Configures a Multiple Spanning Tee Protocol (MSTP) instance that allows multiple VLANs to be managed by a single STP instance and supports per-VLAN STP. This allows you to use fewer spanning-tree instances to map to VLANs.

Syntax

mstp instance *number* { **priority** *priority-num* | **vlan** *vlan-id* [**to** *vlan-id*] | **vlan-group** *group-id* | **ethernet** *stackid/slot/port* { **path-cost** *cost-value* [**priority** *priority-value*] | **priority** *priority-value* [**path-cost** *cost-value*]}

no mstp instance *number* { **priority** *priority-num* | **vlan** *vlan-id* [**to** *vlan-id*] | **vlan-group** *group-id* | **ethernet** *stackid/slot/port* { **path-cost** *cost-value* [**priority** *priority-value*] | **priority** *priority-value* [**path-cost** *cost-value*]}

Command Default

No MSTP instances are configured. Any VLANs remain in the common, internal spanning tree (CIST) or are free.

Parameters

number

Specifies the number for the instance of MSTP that you are configuring. You can specify up to 15 instances, identifying each, in MSTP mode, by a number in the range 1 through 4094. In MSTP mode, you cannot specify the value 0, which identifies the CIST. In MSTP+ mode, the range is 0 through 4094.

priority *priority-num*

Configures the priority for an MSTP instance. Valid values are from 0 through 61440 in increments of 4096. The default value is 32768.

vlan *vlan-id*

Assigns one or more VLANs or a range of VLANs to the MSTP instance.

to *vlan-id*

Assigns a range of VLANs to the MSTP instance.

vlan-group *group-id*

Assigns one or more VLAN groups to the MSTP instance.

ethernet *stackid/slot/port*

Configures port parameters for the MSTP instance.

path-cost *cost-value*

Configures MSTP port path cost. Valid values are from 1 through 200000000.

priority *priority-value*

Specifies the forwarding preference for instances within a VLAN or on the device. You can specify a numeric value in the range 0 to 61440 in increments of 4096. A higher priority variable means a lower forwarding priority. The default value is 32768.

Modes

Global configuration mode

Usage Guidelines

The Brocade implementation of MSTP allows you to assign VLANS or ranges of VLANs to an MSTP instance before or after they have been defined. If predefined, a VLAN will be placed in the MSTI that it was assigned to immediately when the VLAN is created. Otherwise, the default operation is to assign all new VLANs to the CIST. VLANs assigned to the CIST by default can be moved later to a specified MSTI.

The system does not allow an MSTI without any VLANs mapped to it. Consequently, removing all VLANs from an MSTI, deletes the MSTI from the system. The CIST by contrast will exist regardless of whether or not any VLANs are assigned to it. Consequently, if all VLANs are moved out of a CIST, the CIST will still exist and remain functional.

You can set a priority to the instance that gives it forwarding preference over lower priority instances within a VLAN or on the switch. A higher number for the priority variable means a lower forwarding priority.

The system does not allow an MSTP instance without any VLANs mapped to it; removing all VLANs from an MSTP instance deletes the instance from the system.

In MSTP+ mode, you can specify an instance number value of 0 because MSTP+ mode allows you to add VLANs to and remove VLANs from the CIST.

In MSTP mode, the **no** form of this command moves a VLAN or VLAN group from its assigned MSTP back into the CIST. In MSTP+ mode, the **no** form of this command assigns any VLAN as a free VLAN.

Examples

The following example configures an MSTP instance and map VLANs 1 to 7 to it.

```
Device(config)# mstp instance 7 vlan 4 to 7
```

The following example specifies a priority of 8192 to MSTP instance 1.

```
Device(config)# mstp instance 1 priority 8192
```

mstp max-age

Configures the amount of time the device waits to receive a Hello packet before it initiates a topology change.

Syntax

mstp max-age *time*

no mstp max-age *time*

Command Default

The default is 20 seconds.

Parameters

time

The time period a device waits to receive a Hello packet before it initiates a topology change. The period ranges from 6 through 40 seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the maximum age to the default value.

Examples

The following example configures the maximum age to 20.

```
device(config)# mstp max-age 20
```

mstp max-hops

Configures the maximum hop count.

Syntax

mstp max-hops *count*

no mstp max-hops *count*

Command Default

The default is 20 hops.

Parameters

count

The maximum hop count. The number of hops ranges from 1 through 40.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the maximum hop count to the default value.

Examples

The following example configures the maximum hop count to 20.

```
device(config)# mstp max-hops 20
```

mstp name

Configures the MSTP name for the device.

Syntax

mstp name *name*

no mstp name *name*

Command Default

The default name for the device is blank (no name).

Parameters

name

The MSTP name for the device.

Modes

Global configuration mode

Usage Guidelines

Each switch that is running MSTP should be configured with a name. The name applies to the switch that can have many different VLANs that can belong to many different MSTP regions.

The **no** form of the command resets the MSTP name to blank (no name).

Examples

The following example configures the MSTP name as Device1.

```
device(config)# mstp name Device1
```

mstp revision

Configures an MSTP revision number for the device.

Syntax

mstp revision *number*

no mstp revision*number*

Command Default

The default MSTP revision number for a device is 0.

Parameters

number

The revision level for MSTP. The MSTP revision number ranges from 0 through 65535.

Modes

Global configuration mode

Usage Guidelines

The MSRP revision number applies to the device that can have many different VLANs that can belong to many different MSTP regions.

The **no** form of the command sets the revision level to 0.

Examples

The following example shows how to set the MSTP revision number for a device.

```
device(config)# mstp revision 4
```

mstp scope

Configures VLANs in Multiple Spanning Tee Protocol (MSTP) mode.

Syntax

mstp scope { **all** | **pvst** }

no mstp scope { **all** | **pvst** }

Command Default

No VLAN is under direct MSTP control.

Parameters

all

Configures MSTP on all VLANs.

pvst

Configures MSTP in per-VLAN spanning tree (PVST) mode.

Modes

Global configuration mode

Usage Guidelines

MSTP is not operational until the **mstp start** command is configured. You cannot start MSTP+ unless at least one MSTP+ instance of MSTP + is configured.

The **no** form of this command removes the MSTP PVST mode and restores the device to non-MSTP mode.

Examples

The following example configures MSTP mode on all VLANs.

```
device(config)# mstp scope all
```

The following example enables MSTP in PVST mode.

```
device(config)# mstp scope pvst
```

History

Release version	Command history
08.0.20	This command was modified to support the **pvst** keyword.

mstp start

Enables MSTP on the device.

Syntax

mstp start

no mstp start

Command Default

MSTP is disabled by default.

Modes

Global configuration mode

Usage Guidelines

MSTP scope must be enabled on the device before MSTP can be enabled.

The **no** form of the command disables MSTP on a device.

Examples

The following example shows how to start MSTP on the device.

```
device(config)# mstp start
```

multicast disable-pimsm-snoop

Disables PIM Sparse mode (SM) snooping for a specific VLAN when snooping is enabled globally.

Syntax

multicast disable-pimsm-snoop

no multicast disable-pimsm-snoop

Command Default

The global PIM SM snooping setting applies.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the global PIM SM snooping setting.

Examples

This example disables PIM SM snooping on VLAN 20.

```
Device(config)#config vlan 20
Device(config-vlan-20)#multicast disable-pimsm-snoop
```

multicast fast-convergence

Configures a device to listen to topology change events in Layer 2 protocols such as spanning tree, and then send general queries to shorten the convergence time.

Syntax

multicast fast-convergence

no multicast fast-convergence

Command Default

Fast convergence is not configured.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default; fast convergence is not configured.

If the Layer 2 protocol cannot detect a topology change, fast convergence may not work in some cases. For example, if the direct connection between two devices switches from one interface to another, the Rapid Spanning Tree protocol (802.1w) considers this optimization rather than a topology change. In this example, other devices do not receive topology change notifications, and cannot send queries to speed up the convergence. Fast convergence works well with the regular spanning tree protocol in this case.

Examples

This example configures fast convergence on VLAN 70.

```
Device(config)#vlan 70
Device(config-vlan-70)#multicast fast-convergence
```

multicast fast-leave-v2

Configures fast leave for IGMP V2.

Syntax

multicast fast-leave-v2

no multicast fast-leave-v2

Command Default

Fast leave for IGMP V2 is not configured.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default; fast leave for IGMP V2 is not configured.

When a device receives an IGMP V2 leave message, it sends out multiple group-specific queries. If no other client replies within the waiting period, the device stops forwarding traffic. When the **multicast fast-leave-v2** command is configured, and when the device receives a leave message, it immediately stops forwarding to that port. The device does not send group specific-queries. When the **multicast fast-leave-v2** command is configured on a VLAN, you must not have multiple clients on any port that is part of the VLAN.

In a scenario where two devices connect, the querier device should not be configured for fast-leave-v2 because the port might have multiple clients through the non-querier.

You can configure the **ip multicast leave-wait-time** command to set the number of queries and the waiting period.

Examples

This example configures fast leave for IGMP on VLAN 10.

```
Device(config)#vlan 10
Device(config-vlan-10)#multicast fast-leave-v2
```

multicast limit

Enables rate limiting on a port, enables Syslog logging of multicast packets, or sets a packet drop threshold value.

Syntax

multicast limit *num* **kbps** [**log** | **threshold** *packet_threshold* **action port-shutdown** [*shutdown_seconds*]]

no multicast limit *num* **kbps** [**log** | **threshold** *packet_threshold* **action port-shutdown** [*shutdown_seconds*]]

Command Default

Multicast rate limiting, logging, and port dampening are disabled.

Parameters

num
: Specifies the maximum number of broadcast packets per second ranging from 1 to 8388607; or when followed by **kbps**, *num* is the number of kilo bits per second (kbps) permitted for byte-based limiting. The value in this case is 1 to the maximum port speed. Use 0 to disable rate limiting.

kbps
: Enables byte-based limiting. The value can be 1 to Max Port Speed.

log
: Enables Syslog logging when the multicast limit exceeds *num* **kpbs** .

threshold
: The packet drop count threshold.

packet_threshold
: Specifies the number of packets (in kilo bytes) that when exceeded, the port is shutdown. The value ranges from 1 KB to 10 GB.

action
: The action to be taken.

port-shutdown
: Set the **action** as a port shutdown event.

shutdown_seconds
: The amount of time, in seconds, the port is shutdown. The default is 300 seconds and the range is from 1 to 65535 seconds.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to disable rate limiting on a port, Syslog logging of excess packets, or the packet drop threshold value.

If the port *shutdown_seconds* parameter is set to 0, the port is kept in ERR-DISABLE state until you re-enabled it.

Examples

The following example enables a multicast rate limit of 131072 kbps.

```
device(config)# interface ethernet 9/1/1
device(config-if-e1000-9/1/1)# multicast limit 131072 kbps
```

The following example enables multicast limit logging when the configured multicast limit exceeds 100 Kbps.

```
device(config)# interface ethernet 1/2/1
device(config-if-e10000-1/2/1)# multicast limit 100 kbps log
```

The following example shuts down the port for 300 seconds (default) when the packet drop threshold value exceeds 1000 KBs.

```
device(config)# interface ethernet 1/2/1
device(config-if-e10000-1/2/1)# multicast limit 100 kbps threshold 1000 action port-shutdown
```

History

Release version	Command history
8.0.10	The command was introduced.
8.0.30h	The command was modified to include the keyword **threshold**.
8.0.40a	The command was modified to include the keyword **log**.

multicast pimsm-snooping prune-wait

Configures the amount of time a device waits after receiving a PIM prune message before removing the outgoing interface (OIF) from the forwarding entry.

Syntax

multicast pimsm-snooping prune-wait *seconds*

no multicast pimsm-snooping prune-wait *seconds*

Command Default

The prune-wait time is 5 seconds.

Parameters

seconds

The time to wait, in seconds. The range is 0 to 65535; the default is 5.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default prune-wait time (5 seconds).

The prune-wait time is necessary on a LAN where multiple receivers could be listening to the group; it gives them time to override the prune message. Configure the **multicast pimsm-snooping prune-wait** command to modify the prune-wait time according to topology and PIM router configurations.

In accordance with RFC 4601, PIM routers delay pruning for 3.5 seconds by default, so configuring a lower prune-wait value may cause traffic disruption. You should configure a prune-wait value lower than 3.5 seconds only if the topology supports it, for example, if the group has only one receiver, and an immediate prune is needed.

Examples

The following example configures the prune-wait time to 7 seconds.

```
Device(config)#vlan 10
Device(config-vlan-10)#multicast pimsm-snooping prune-wait 7
```

History

Release version	Command history
8.0.20	This command was introduced.

multicast port-version

Configures the IGMP version on individual ports in a VLAN.

Syntax

multicast port-version { **2** | **3** } **ethernet** *port* [**ethernet** *port* | **to** *port*]

no multicast port-version { **2** | **3** } **ethernet** *port* [**ethernet** *port* | **to** *port*]

Command Default

The port uses the IGMP version configured globally or for the VLAN.

Parameters

2

Configures IGMP version 2.

3

Configures IGMP version 3.

ethernet *port*

Specifies the port to configure the version on.

to

Specifies a range of ports.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the IGMP version configured globally or for the VLAN.

You can specify a list of ports, separated by a space, or a range of ports, or you can combine lists and ranges.

See the description of the **ip multicast version** command for information on how to configure the IGMP version globally.

See the description of the **multicast version** command for information on how to configure the IGMP version on a VLAN.

Examples

This example configures ports 4, 5, and 6 to use IGMP version 3.

```
Device(config)#config vlan 20
(config-vlan-20)#multicast port-version 3 ethernet 2/4 to 2/6
```

multicast proxy-off

Turns off proxy activity for static groups.

Syntax

multicast proxy-off

no multicast proxy-off

Command Default

Proxy activity is on.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default; proxy activity is on.

When a device is configured for static groups, it acts as a proxy and sends membership reports for the static groups when it receives general or group-specific queries. When a static group configuration is removed, the group is deleted from the active group table immediately. However, leave messages are not sent to the querier, and the querier must age out the group. You can configure the **multicast proxy-off** command to turn off proxy activity.

Examples

This example turns off proxy activity for VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast proxy-off
```

multicast router-port

Configures a static router Ethernet port to receive multicast control and data packets.

Syntax

multicast router-port ethernet *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/portnum*]

multicast router-port ethernet *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/portnum*]

Command Default

The device forwards all multicast control and data packets only to router ports that receive queries.

Parameters

stackid/slot/portnum

Specifies the Ethernet port you want to force traffic to. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id. You can configure a single port or a list of ports, separated by a space.

to

Specifies a range of ports.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default, that is, the device forwards all multicast control and data packets only to router ports that receive queries.

Examples

This example configures a static port on Ethernet 1/1/3 on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/3
```

This example configures a list of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/24 ethernet 1/6/24 ethernet 1/8/17
```

This example configures a range of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/1 to 1/1/8
```

This example configures a combined range and list of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast router-port ethernet 1/1/1 to 1/1/8 ethernet 1/1/24 ethernet 1/6/24
ethernet 1/8/17
```

multicast static-group

Configures a static IGMP group for a VLAN.

Syntax

multicast static-group *ipv4-address* [**count** *num*] [**ethernet** *stackid/slot/portnum* | **drop**]

no multicast static-group *ipv4-address* [**count** *num*] [**ethernet** *stackid/slot/portnum* | **drop**]

Command Default

The VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports.

Parameters

ipv4-address
: Specifies the address of the static group.

count *num*
: Specifies a contiguous range of groups.

ethernet *stackid/slot/portnum*
: Specifies the ports to be included in the group. On standalone devices specify the interface ID in the format slot/port-iD; on stacked devices you must also specify the stack ID, in the format stack-ID/slot/port-ID.

drop
: Specifies discarding data traffic to a group in hardware.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command removes the static group fromr the VLAN.

A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports. You can configure the **multicast static-group** command to create a static group that applies to specific ports, allowing packets to be forwarded to them even though they have no client membership reports.

On FCX, ICX 6610, ICX 6430, ICX 6450, and ICX 6650 devices, configuring the **drop** keyword discards data traffic to a group in hardware. The group can be any multicast group including groups in the reserved range of 224.0.0.X. Configuring the **drop** keyword does not affect IGMP packets, which are always trapped to CPU when snooping is enabled. It applies to the entire VLAN, and cannot be configured for a port list. When the **drop** keyword is not configured, the group must exist outside the reserved range.

Examples

This example configures on VLAN 20 a static group containing ports 1/1/3 and 1/1/5 to 1/1/7.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# multicast static-group 224.1.1.1 count 2 ethernet 1/1/3 ethernet 1/1/5 to 1/1/7
```

multicast tracking

Enables tracking and fast leave on VLANs.

Syntax

multicast tracking

no multicast tracking

Command Default

Tracking and fast leave are disabled.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default, that is, tracking and fast leave are disabled.

The membership tracking and fast leave features are supported for IGMP V3 only. If any port or any client is not configured for IGMP V3, the multicast tracking command is ignored.

Examples

This example enables tracking and fast leave on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast tracking
```

multicast version

Configures the IGMP version for snooping on a VLAN.

Syntax

multicast version [**2** | **3**]

no multicast version

Command Default

The globally-configured IGMP version is used.

Parameters

2

Configures IGMP version 2.

3

Configures IGMP version 3.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the globally configured version.

If an IGMP version is configured for an individual port, that port uses the version configured for it, not the VLAN version.

See the description of the **ip multicast version** command for information on how to configure the IGMP version globally.

See the description of the **multicast port-version** command for information on how to configure the IGMP version on an individual port

Examples

This example configures IGMP version 3 on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast version 3
```

multicast6 disable-mld-snoop

Disables multicast listening discovery (MLD) snooping for a specific VLAN when snooping is enabled globally.

Syntax

multicast6 disable-multicast-snoop

no multicast6 disable-multicast-snoop

Command Default

The global MLD snooping setting applies.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the global MLD snooping setting.

Examples

This example disables MLD snooping on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 disable-multicast-snoop
```

multicast6 disable-pimsm-snoop

When PIM6 SM snooping is enabled globally, overrides the global setting and disables it for a specific VLAN.

Syntax

multicast6 disable-pimsm-snoop

no multicast6 disable-pimsm-snoop

Command Default

The globally configured PIM6 SM snooping applies.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the globally configured PIM6 SM snooping.

The device must be in multicast listening discovery (MLD) passive mode before PIM6 SM snooping can be disabled.

Examples

This example enables PIM6 SM traffic snooping on VLAN 20.

```
Device(config)# vlan 20
Device(config-vlan-20)#multicast6 disable-pimsm-snoop
```

multicast6 fast-convergence

Configures a device to listen to topology change events in Layer 2 protocols such as spanning tree, and then send general queries to shorten the convergence time.

Syntax

multicast6 fast-convergence

no multicast6 fast-convergence

Command Default

Fast convergence is not configured.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default; fast convergence is not configured.

Configure the **multicast6 fast-convergence** command to allow a device to listen to topology change events in Layer 2 protocols, such as Spanning Tree, and send general queries to shorten the convergence time.

If the Layer 2 protocol cannot detect a topology change, fast convergence may not work in some cases. For example, if the direct connection between two devices switches from one interface to another, the Rapid Spanning Tree protocol (802.1w) considers this to be optimization rather than a topology change. In this case, other devices do not receive topology change notifications and cannot send queries to speed up convergence. The original spanning tree protocol does not recognize optimization actions, and fast convergence works in all cases.

Examples

This example configures fast convergence on VLAN 70.

```
device# configure terminal
device(config)# vlan 70
device(config-vlan-70)# multicast6 fast-convergence
```

multicast6 port-version

Configures the multicast listening discovery (MLD) version on individual ports in a VLAN.

Syntax

multicast6 port-version { **1** | **2** } [**ethernet** *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *port*]]

no multicast6 port-version { **1** | **2** } [**ethernet** *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *port*]]

Command Default

The port uses the MLD version configured globally or for the VLAN.

Parameters

1

Configures MLD version 1.

2

Configures MLD version 2.

ethernet *stackid/slot/portnum*

Specifies the port to configure the version on. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id. You can specify a list of ports, separated by a space, or a range of ports, or you can combine lists and ranges.

to

Specifies a range of ports.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the MLD version configured globally or for the VLAN.

When you configure the MLD version on a specified port or range of ports, the other ports use the MLD version specified with the **multicast6 version** command, or the globally configured MLD version.

Examples

This example configures ports 1/1/4, 1/1/5, 1/1/6, and 1/2/1 on VLAN 20 to use MLD version 2.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 port-version 2 ethernet 1/2/1 ethernet 1/1/4 to 1/1/6
```

multicast6 proxy-off

Turns off multicast listening discovery (MLD) proxy activity.

Syntax

multicast6 proxy-off

no multicast6 proxy-off

Command Default

MLD snooping proxy activity is on.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default; proxy activity is on.

When a device is configured for static groups, it acts as a proxy and sends membership reports for the static groups when it receives general or group-specific queries. When a static group configuration is removed, the group is deleted from the active group table immediately. However, leave messages are not sent to the querier, and the querier must age out the group. You can configure the **multicast proxy-off** command to turn off proxy activity.

Examples

This example turns off proxy activity for VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 proxy-off
```

multicast6 router-port

Configures a static router port to receive IPv6 multicast control and data packets.

Syntax

multicast6 router-port ethernet *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/portnum*]

no multicast6 router-port ethernet *stackid/slot/portnum* [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/portnum*]

Command Default

The device forwards all IPv6 multicast control and data packets only to router ports that receive queries.

Parameters

ethernet *stackid/slot/portnum*

Specifies the Ethernet port you want to force traffic to. On standalone devices specify the interface ID in the format slot/port-ID; on stacked devices you must also specify the stack ID, in the format stack-ID/slot/port-ID. You can configure a single port or a list of ports, separated by a space.

to

Specifies a range of ports.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default, that is, the device forwards all multicast control and data packets only to router ports that receive queries.

All multicast control and data packets are forwarded to router ports that receive queries. Although router ports are learned, you can configure static router ports to force multicast traffic to specific ports, even though these ports never receive queries.

Examples

This example configures a range and a list of static ports on VLAN 70.

```
device#configure terminal
device(config)#vlan 70
device(config-vlan-70)#multicast6 router-port ethernet 1/1/1 to 1/1/8 ethernet 1/1/24 ethernet 1/6/24
ethernet 1/8/17
```

multicast6 static-group

Configures a static multicast listening discovery (MLD) group for a VLAN.

Syntax

multicast6 static-group *ipv6-address* [**count** *num*] [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/ portnum*]

no multicast6 static-group *ipv6-address* [**count** *num*] [**ethernet** *stackid/slot/portnum* | **to** *stackid/slot/ portnum*]

Command Default

The VLAN cannot forward multicast traffic to ports that do not receive MLD membership reports.

Parameters

ipv6-address

Specifies the IPv6 address of the multicast group.

count *num*

Specifies a contiguous range of groups. The default is 1.

to

Specifies a range of ports.

ethernet *stackid/slot/portnum*

Specifies the Ethernet port you want to force traffic to. On standalone devices specify the interface ID in the format slot/port-ID; on stacked devices you must also specify the stack ID, in the format stack-ID/slot/port-ID. You can configure a single port or a list of ports, separated by a space.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command removes the static group fromr the VLAN.

A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive MLD membership reports. To allow clients to send reports, you can configure a static group that applies to individual ports on the VLAN. The static group forwards packets to the static group ports even if they have no client membership reports.

You cannot configure a static group that applies to an entire VLAN.

The maximum number of supported static groups in a VLAN is 512, and the maximum number of supported static groups for individual ports in a VLAN is 256.

Examples

This example configures on VLAN 20 a static group containing ports 0/1/3 and 0/1/5 to 0/1/7.

```
Device(config)#vlan 20
(config-vlan-20)#multicast6 static-group ff05::100 count 2 ethernet 0/1/3 ethernet 0/1/5 to 0/1/7
```

multicast6 tracking

Enables tracking and fast leave for IPv6 multicast listening discovery Version 2 (MLDv2) on VLANs.

Syntax

multicast6 tracking

no multicast6 tracking

Command Default

Tracking and fast leave are disabled.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of this command restores the default, that is, tracking and fast leave are disabled.

The membership tracking and fast leave features are supported for MLDv2 only. If any port or any client is not configured for MLDv2, the multicast tracking command is ignored.

Examples

This example enables tracking and fast leave on VLAN 20.

```
Device(config)#vlan 20
Device(config-vlan-20)#multicast6 tracking
```

multicast6 version

Configures the multicast listening discovery (MLD) version for snooping on a VLAN.

Syntax

multicast6 version { **1** | **2** }

no multicast6 version { **1** | **2** }

Command Default

The globally configured MLD version is configured.

Parameters

1

Configures MLD Version 1.

2

Configures MLD Version 2.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the globally configured MLD version.

If an MLD version is specified for individual ports, these ports use that version instead of the version specified for the VLAN.

Examples

This example specifies MLD Version 2 on VLAN 20.

```
Device(config)# vlan 20
Device(config-vlan-20)#multicast6 version 2
```

multipath

Changes load sharing to apply to only IBGP or EBGP paths, or to support load sharing among paths from different neighboring autonomous systems.

Syntax

multipath { **ebgp** | **ibgp** | **multi-as** }

no multipath { **ebgp** | **ibgp** | **multi-as** }

Command Default

This option is disabled.

Parameters

ebgp

Enables load sharing of EBGP paths only.

ibgp

Enables load sharing of IBGP paths only.

multi-as

Enables load sharing of paths from different neighboring autonomous systems.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

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.

By default, when BGP4 load sharing is enabled, both IBGP and EBGP paths are eligible for load sharing, while paths from different neighboring autonomous systems are not.

Examples

This example changes load sharing to apply to IBGP paths in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# multipath ibgp
```

This example enables load sharing of paths from different neighboring autonomous systems in the IPv6 address family.

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

This example changes load sharing to apply to EBGP paths in a nondefault VRF instance in the IPv4 address family.

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

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

name (MRP)

Configures the name for the metro ring.

Syntax

name *string*

no name *string*

Command Default

Metro ring names are not configured.

Parameters

string

Specifies the name for the metro ring. The name is an ASCII string and can be up to 64 characters in length and include blank spaces.

Modes

MRP configuration mode

Usage Guidelines

The name is optional for a metro ring. If you use a name that has blank spaces, enclose the name in double quotation marks, for example, "Customer A".

The **no** form of the command removes the name for the metro ring.

Examples

The following example configures the name for a metro ring.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)# name CustomerA
```

nbr-timeout

Configures the interval after which a PIM device considers a neighbor to be absent.

Syntax

nbr-timeout *seconds*

no nbr-timeout *seconds*

Command Default

The timeout interval is 105 seconds.

Parameters

seconds

Specifies the interval, in seconds. The range is 35 through 65535 seconds. The default is 105 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the default timeout interval, 105 seconds.

You should set the interval to be not less than 3.5 times the hello timer value.

Examples

This example configures a PIM neighbor timeout value of 360 seconds on all ports on a device operating with PIM.

```
Device(config)# router pim
Device(config-pim-router)# nbr-timeout 360
```

neighbor activate

Enables the exchange of information with BGP neighbors and peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

Command Default

Enabling address exchange for the IPv6 address family is disabled.

Parameters

ip-address
Specifies the IPv4 address of the neighbor.

ipv6-address
Specifies the IPv6 address of the neighbor.

peer-group-name
Specifies a peer group.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable the exchange of an address with a BGP neighbor or peer group.

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.

Examples

This example establishes a BGP session with a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 neighbor activate
```

This example establishes a BGP session with a neighbor with the IPv6 address 2001:2018:8192::125 for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 neighbor activate
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor advertisement-interval

Enables changes to the interval over which a specified neighbor or peer group holds route updates before forwarding them.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval** *seconds*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval**

Command Default

The default is 0.

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

seconds
: Range is from 0 through 3600.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Examples

This example changes the BGP4 advertisement interval from the default to 60 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 advertisement-interval 60
```

This example changes the BGP4+ advertisement interval from the default for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 advertisement-interval 60
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor allowas-in

Disables the AS_PATH check function for routes learned from a specified location so that BGP does not reject routes that contain the recipient BGP speaker's AS number.

Syntax

neighbor {*ip-address* | *ipv6-address* | *peer-group-name* } **neighbor allowas-in** *number*

no neighbor allowas-in {*ip-address* | *ipv6-address* | *peer-group-name* } **neighbor allowas-in** *number*

Command Default

The AS_PATH check function is enabled and any route whose path contains the speaker's AS number is rejected as a loop.

Parameters

ip-address
: Specifies the IP address of the neighbor.

ipv6-address
: Specifies the IPv6 address of the neighbor.

peer-group-name
: Specifies a peer group.

number
: Specifies the number of times that the AS path of a received route may contain the recipient BGP speaker's AS number and still be accepted. Valid values are 1 through 10.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to re-enable the AS_PATH check function.

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.

Examples

This example specifies that the AS path of a received route may contain the recipient BGP speaker's AS number three times and still be accepted.

```
device#configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 allowas-in 3
```

neighbor as-override

Replaces the autonomous system number (ASN) of the originating device with the ASN of the sending BGP device.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

Usage Guidelines

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

BGP loop prevention verifies the ASN in the AS path. If the receiving router sees its own ASN in the AS path of the received BGP packet, the packet is dropped. The receiving router assumes that the packet originated from its own AS and has reached the place of origination. This can be a significant problem if the same ASN is used among various sites, preventing sites with identical ASNs from being linked by another ASN. In this case, routing updates are dropped when another site receives them.

Examples

This example replaces the ASN globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 as-override
```

neighbor capability as4

Enables or disables support for 4-byte autonomous system numbers (ASNs) at the neighbor or peer-group level.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**enable** | **disable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**enable** | **disable**]

Command Default

4-byte ASNs are disabled by default.

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor .

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

enable
: Enables 4-byte numbering.

disable
: Disables 4-byte numbering.

Modes

BGP configuration mode

Usage Guidelines

Use the **disable** keyword or the **no** form of this command to remove all neighbor capability for 4-byte ASNs.

4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

Examples

This example enables 4-byte ASNs globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 capability as4 enable
```

neighbor capability orf prefixlist

Advertises outbound route filter (ORF) capabilities to peer routers.

Syntax

neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

no neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

Command Default

ORF capabilities are not advertised to a peer device.

Parameters

ip_address
: Specifies the IPv4 address of the neighbor.

ipv6_address
: Specifies the IPv6 address of the neighbor.

peer-group-name
: Specifies a peer group.

receive
: Enables the ORF prefix list capability in receive mode.

send
: Enables the ORF prefix list capability in send mode.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable ORF capabilities.

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.

Examples

This example advertises the ORF send capability to a neighbor with the IP address 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 capability orf prefixlist send
```

This example advertises the ORF receive capability to a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 capability orf prefixlist receive
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor default-originate

Configures the device to send the default route 0.0.0.0 to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *map-name*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *map-name*]

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

route-map
Optionally injects the default route conditionally, depending on the match conditions in the route map.

map-name
Name of the route map.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This example sends the default route to a BGP4 neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 default-originate route-map myroutemap
```

This example sends the default route to a BGP4+ 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 default-originate route-map myroutemap22
```

neighbor description

Specifies a name for a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **description** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **description**

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

description *string*
: Specifies the name of the neighbor, an alphanumeric string up to 220 characters long.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Examples

This example specifies a BGP4 neighbor name.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 description mygoodneighbor
```

This example specifies a BGP4+ neighbor name for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 default-originate route-map myroutemap
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor ebgp-btsh

Enables EBGP TTL security hack protection (BTSH).

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-btsh**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-btsh**

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Examples

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 ebgp-btsh
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor ebgp-multihop

Allows EBGP neighbors that are not on directly connected networks and sets an optional maximum hop count.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multiphop** [*max-hop-count*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multiphop** [ ]

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

max-hop-count
: Maximum hop count (optional). Range is from 1 through 255.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Examples

This example enables EBGP multihop and sets the maximum hop count to 20.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 ebgp-multihop 20
```

This example enables BGP4+ EBGP multihop for VRF instance "red" and sets the maximum hop count to 40.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 ebgp-multihop 40
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor enforce-first-as

Ensures that a device requires the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGP neighbors to be the ASN of the neighbor that sent the update.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**enable** | **disable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**enable** | **disable**]

Command Default

Disabled by default.

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

enable
: Enables this feature.

disable
: Disables this feature.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to disable this requirement globally for the device.

Examples

This example enables the enforce-first-as feature for a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 enforce-first-as enable
```

neighbor filter-list

Specifies a filter list to be applied to updates from or to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

ip-prefix-list-name
: Name of the filter list.

in
: Specifies that the list is applied on updates received from the neighbor.

out
: Specifies that the list is applied on updates sent to the neighbor.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This example specifies that filter list “myfilterlist” be applied to updates to a neighbor with the IP address 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 filter-list myfilterlist out
```

This example specifies that filter list “2” be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 filter-list 2 in
```

neighbor local-as

Causes the device to prepend the local autonomous system number (ASN) automatically to routes received from an EBGP peer.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

num
: Local ASN. Range is from 1 through 4294967295.

no-prepend
: Causes the device to stop prepending the selected ASN.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the local ASN.

Examples

This example ensures that a device prepends the local ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100
```

This example stops the device from prepending the selected ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100 no-prepend
```

neighbor maxas-limit in

Causes the device to discard routes received in UPDATE messages if those routes exceed a maximum AS path length.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in** { *num* | **disable** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in**

Command Default

This command is disabled by default.

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

num
: Maximum length of the AS path. Range is from 0 through 300. The default is 300.

disable
: Prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead uses the default system value.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration.

Examples

This example changes the length of the maximum allowed AS path length from the default.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 maxas-limit in 200
```

This example prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead use the default system value.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 maxas-limit in disable
```

neighbor maximum-prefix

Specifies the maximum number of IP network prefixes (routes) that can be learned from a specified neighbor or peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**]

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

num
: Maximum number of IP prefixes that can be learned. Range is from 0 through 4294967295. Default is 0 (unlimited).

threshold
: Specifies the percentage of the value specified by *num* that causes a syslog message to be generated. Range is from 1 through 100. Default is 100.

teardown
: Tears down the neighbor session if the maximum number of IP prefixes is exceeded.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This example sets the maximum number of prefixes that will be accepted from the neighbor with the IP address 10.11.12.13 to 100000, and sets the threshold value to 80%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)#  neighbor 10.11.12.13 maximum-prefix 100000 threshold 80
```

neighbor next-hop-self

Causes the device to list itself as the next hop in updates that are sent to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

always
: Enables this feature for route reflector (RR) routes.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration.

Examples

This example causes all updates destined for the neighbor with the IP address 10.11.12.13 to advertise this device as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 next-hop-self
```

This example, for the VRF instance "red," causes all updates destined for the neighbor with the IPv6 address 2001:2018:8192::125 to advertise this device as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 next-hop-self
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor password

Specifies an MD5 password for securing sessions between the device and a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password**

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor.

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

string
: Password of up to 63 characters in length that can contain any alphanumeric character.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration.

Examples

This example specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 password s0M3P@55W0Rd
```

This BGP4+ example, for VRF instance "red," specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 2001:2018:8192::125 password s0M3P@55W0Rd
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor peer-group

Configures a BGP neighbor to be a member of a peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* } **peer-group** *string*

no neighbor { *ip-address* | *ipv6-address* } **peer-group** *string*

Parameters

ip-address
IPv4 address of the neighbor.

ipv6-address
IPv6 address of the neighbor.

peer-group *string*
Specifies the name of a BGP peer group. The name can be up to 63 characters in length and can be composed of any alphanumeric character.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove a neighbor from the peer group.

Examples

This example assigns a specified neighbor to a peer group called “mypeergroup1”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 peer-group mypeergroup1
```

This BGP4+ example, for VRF instance "red," assigns a specified neighbor to a peer group called "mypeergroup1".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u)# neighbor 2001:2018:8192::125 peer-group mypeergroup1
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor prefix-list

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to IP address and mask length.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

string
: Name of the prefix list.

in
: Applies the filter in incoming routes.

out
: Applies the filter in outgoing routes.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This example applies the prefix list "myprefixlist" to incoming advertisements to neighbor 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 prefix-list myprefixlist in
```

This example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

neighbor remote-as

Specifies the autonomous system (AS) in which a remote neighbor resides.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as**

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

num
: Remote AS number (ASN). Range is from 1 through 4294967295.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove the neighbor from the AS.

Examples

This example specifies AS 100 for a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor 10.11.12.13 remote-as 100
```

The following BGP4+ example, for VRF instance "red," specifies AS 100 for a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 remote-as 100
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor remove-private-as

Configures a device to remove private autonomous system numbers (ASNs) from UPDATE messages that the device sends to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

The device will remove ASNs 64512 through 65535 (the well-known BGP4 private ASNs) from the AS-path attribute in UPDATE messages that the device sends to a neighbor.

Examples

This example removes private ASNs globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remove-private-as
```

This example removes private ASNs for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 remove-private-as
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor route-map

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to a set of attributes defined in a route map.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

in
: Applies the filter on incoming routes.

string
: Name of the route map.

out
: Applies the filter on outgoing routes.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This example applies a route map named "myroutemap" to an outgoing route from 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 route-map myroutemap out
```

neighbor route-reflector-client

Configures a neighbor to be a route-reflector client.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

Parameters

ip-address
IPv4 address of the neighbor

ipv6-address
IPv6 address of the neighbor

peer-group-name
Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Use this command on a host device to configure a neighbor to be a route-reflector client. Once configured, the host device from which the configuration is made acts as a route-reflector server.

Examples

This example configures a neighbor to be a route-reflector client.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 route-reflector-client
```

neighbor send-community

Enables sending the community attribute in updates to the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]

Command Default

The device does not send community attributes.

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

both
: Sends both standard and extended attributes.

extended
: Sends extended attributes.

standard
: Sends standard attributes.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This example sends standard community attributes to a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 send-community standard
```

neighbor shutdown

Causes a device to shut down the session administratively with its BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown** { **generate-rib-out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown** { **generate-rib-out** }

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

generate-rib-out
: When a peer is put into the shutdown state, Routing Information Base (RIB) outbound routes are not produced for that peer. Use this option to produce those routes.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Shutting down a session lets you configure the neighbor and save the configuration without the need to establish a session with that neighbor.

Examples

This example a device to shut down the session administratively with its neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 shutdown
```

This example causes a device to shut down the session administratively with its neighbor and generate RIB outbound routes for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 shutdown generate-rib-out
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor soft-reconfiguration inbound

Stores all the route updates received from a BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Soft reconfiguration stores all the route updates received from a neighbor. If you request a soft reset of inbound routes, the software compares the policies against the stored route updates, instead of requesting the neighbor's BGP4 or BGP4+ route table or resetting the session with the neighbor.

Examples

This example globally stores route updates from a BGP4 neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 soft-configuration inbound
```

This example stores route updates from a BGP4+ neighbor for VRF instance "red".

```
device# configure terminal
device(config)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 soft-configuration inbound
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor timers

Specifies how frequently a device sends KEEPALIVE messages to its BGP neighbors, as well as how long the device waits for KEEPALIVE or UPDATE messages before concluding that a neighbor is dead.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *keepalive_interval* **hold-time** *holdtime_interval*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *keepalive_interval* **hold-time** *holdtime_interval*

Command Default

The keep-alive timer is 60 seconds. The hold timer is 180 seconds.

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

keep-alive *keepalive_interval*
: Frequency (in seconds) with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

hold-time *holdtime_interval*
: Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Examples

This example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

This example sets the keepalive timer for VRF instance "red" to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor update-source

Configures the device to communicate with a neighbor through a specified interface.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address* | *ipv6-address* | **ethernet** | **loopback** *num* | **ve** *vlan_id* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address* | *ipv6-address* | **ethernet** | **loopback** *num* | **ve** *vlan_id* }

Parameters

ip-address
: IPv4 address of the neighbor

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Peer group name configured by the **neighbor** *peer-group-name* command.

ip-address
: IP address of the update source.

ipv6-address
: IPv6 address of the update source.

ethernet *stackid/slot/portnum*
: Specifies the physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *num*
: Specifies a loopback interface.

ve *vlan_id*
: Specifies a virtual Ethernet VLAN interface.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

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

Examples

This example configures the device globally to communicate with a neighbor through the specified IPv4 address and port.

```
device#configure terminal
device#(config)# router bgp
device(config-bgp)# neighbor 10.11.12.13 update-source ethernet 15/1/1
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

neighbor weight

Specifies a weight that the device will add to routes that are received from the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight** *num*

Command Default

The default for *num* is 0.

Parameters

ip-address
: IPv4 address of the neighbor.

ipv6-address
: IPv6 address of the neighbor

peer-group-name
: Name of the peer group.

num
: Value from 1 through 65535.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

BGP prefers larger weights over smaller weights.

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.

Examples

This example changes the weight from the default.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 weight 100
```

netbios-name-server

Specifies the IP address of a NetBIOS WINS server or servers available to Microsoft DHCP clients.

Syntax

netbios-name-server *address* [*address2*,*address3*]

Parameters

address

Specifies the IP address of the NetBIOS WINS server.

Modes

DHCP server pool configuration mode.

Examples

The following example specifies the IP address of a NetBIOS WINS server.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# netbios-name-server 192.168.1.55
```

netbios-proto

Configures the NetBIOS protocol-based VLAN and enters NetBIOS protocol VLAN configuration mode.

Syntax

netbios-proto [**name** *string*]

no netbios-proto [**name** *string*]

Command Default

An NetBIOS protocol-based VLAN is not configured.

Parameters

name *string*

Specifies the name of the NetBIOS protocol configuration. The name can be up to 32 characters in length.

Modes

VLAN configuration mode

IP protocol VLAN configuration mode

IPX protocol VLAN configuration mode

IPv6 protocol VLAN configuration mode

DECnet protocol VLAN configuration mode

AppleTalk protocol VLAN configuration mode

Other protocol VLAN configuration mode

Usage Guidelines

The **no** form of the command disables the NetBIOS protocol-based VLANs.

Examples

The following example shows how to configure the NetBIOS protocol-based VLAN.

```
device(config)# ipx-proto name Brown
device(config-vlan-ipx-proto)# netbios-proto name proto1
device(config-vlan-netbios-proto)# no dynamic
```

network

Configures the device to advertise a network.

Syntax

network *network/mask* [**backdoor** | **route-map** *map-name* | **weight** *num*]

no network *network/mask* [**backdoor** | **route-map** *map-name* | **weight** *num*]

Command Default

No network is advertised.

Parameters

network/mask
: Network and mask in CIDR notation.

backdoor
: Changes administrative distance of the route to this network from the EBGP administrative distance (the default is 20) to the local BGP4 weight (the default is 200), tagging the route as a backdoor route.

route-map *map-name*
: Specifies a route map with which to set or change BGP4 attributes for the network to be advertised.

weight*num*
: Specifies a weight to be added to routes to this network. Range is 0 through 65535. The default is 0.

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

Usage Guidelines

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

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.

Examples

This example imports the IPv4 network 10.11.12.12/30 into the route map "myroutemap".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# network 10.11.12.13/30 route-map myroutemap
```

This example imports the IPv6 prefix 2001:db8::/32 into the BGP4+ database and sets a weight of 300.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# network 2001:db8::/32 weight 300
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

network (dhcp)

Configures the subnet network and mask of the DHCP address pool.

Syntax

network *subnet/mask*

Parameters

subnet/mask

Specifies the subnet network and mask of the address pool.

Modes

DHCP server pool configuration mode

Examples

The following command specifies the subnet network and mask of the DHCP address pool.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# network 10.2.3.44/24
```

next-bootstrap-server

Specifies the IP address of the next server the client should use for bootup.

Syntax

next-bootstrap-server *ip-address*

Parameters

ip-address

Specifies the IP address of the next bootstrap server.

Modes

DHCP server pool configuration mode.

Examples

The following example specifies the next bootstrap server.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# next-bootstrap-server 10.2.5.44
```

next-hop-enable-default

Configures the device to use the default route as the next hop.

Syntax

next-hop-enable-default

no next-hop-enable-default

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

Examples

This BGP4 example configures the device to use the default route as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# next-hop-enable-default
```

This BGP4+ example configures the device to use the default route as the next hop.

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

next-hop-recursion

Enables BGP recursive next-hop lookups.

Syntax

next-hop-recursion

no next-hop-recursion

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

If the BGP next hop is not the immediate next hop, a recursive route lookup in the IP routing information base (RIB) is needed. With recursion, a second routing lookup is required to resolve the exit path for destination traffic. Use this command to enable recursive next-hop lookups.

Examples

This example enables recursive next-hop lookups for BGP4.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# next-hop-recursion
```

This BGP4+ example enables recursive next-hop lookups for BGP4+.

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

no-dynamic-aging

Disables aging of ports that are dynamically assigned to the protocol or subnet-based VLANs.

Syntax

no-dynamic-aging

no no-dynamic-aging

Command Default

The dynamic protocol VLAN ages out after 10 or 20 minutes, if no packets are received.

Modes

IP protocol VLAN configuration mode

IPX protocol VLAN configuration mode

AppleTalk protocol VLAN configuration mode

DECnet protocol VLAN configuration mode

NetBIOS protocol VLAN configuration mode

Other protocol VLAN configuration mode

IPV-6 protocol VLAN configuration mode

Usage Guidelines

NOTE
Configure the command only if your configuration includes dynamically assigned VLAN memberships for protocol or subnet VLANs.

The **no** form of the command enables aging of the dynamic protocol VLAN.

Examples

The following example shows how to configure dynamic aging.

```
device(config)# vlan 10 by port
device(config-vlan-10)# interface ethernet 1/1/1 to 1/1/5
device(config-vlan-10)# ip-proto name IP_Prot_VLAN
device(config-vlan-ip-proto)# no-dynamic-aging
```

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
```

ntp

Enables the NTP client and server mode.

Syntax

ntp

no ntp

Command Default

NTP services are disabled on all interfaces by default.

Modes

Global configuration mode

Usage Guidelines

Before you begin to configure NTP, you must use the clock set command to set the time on your device to within 1000 seconds of the coordinated Universal Time (UTC).

Disable SNTP by removing all the SNTP configurations.

> **NOTE**
> NTP and SNTP implementations cannot operate simultaneously. You cannot configure the **ntp** command if SNTP is enabled. If SNTP is enabled, configuring the **ntp** command will display the following message: "SNTP is enabled. Disable SNTP before using NTP for time synchronization"

The **no** form of the command disables the NTP and removes the NTP configuration. The **no ntp** command removes all the configuration which are configured statistically and learned associations from NTP neighbors.

Examples

The following example shows how to enable NTP client and server mode.

```
device(config)# ntp
device(config-ntp)#
```

ntp-interface

Enters NTP interface configuration mode.

Syntax

ntp-interface { **management** *port* | **ethernet** *stackid/slot/port* | **ve** *id* }

no ntp-interface { **management** *port* | **ethernet** *stackid/slot/port* | **ve** *id* }

Parameters

management *port*
: Specifies the management interface.

ethernet *stackid/slot/port*
: Specifies the Ethernet interface.

ve *id*
: Specifies the Virtual Ethernet interface.

Modes

NTP configuration mode

Usage Guidelines

The broadcast server or client is configured on selected interfaces. To remove the NTP broadcast configurations on the specified interface, use the **no** form of this command.

The **no** form of the command to go back to the NTP configuration mode.

The **ntp-interface** command is a mode change command.

Examples

The following example shows how to enter the NTP interface configuration mode for Ethernet 1/1/1.

```
device(config)# ntp
device(config-ntp)# ntp-interface ethernet 1/1/1
device(config-ntp-if-e1000-1/1/1)#
```

The following example shows how to enter the NTP interface configuration mode for management interface 1.

```
device(config)# ntp
device(config-ntp)# ntp-interface management 1
device(config-ntp-mgmt-1)# exit
```

openflow controller

Connects devices to openflow controller connections.

Syntax

openflow controller *ip-address*

openflow controller passive no-ssl

no openflow controller *ip-address*

no openflow controller passive no-ssl

Command Default

The openflow controller is not enabled.

Parameters

ip-address

Specifies the IPv4 address.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the **openflow controller** *ip-address* and **openflow controller passive no-ssl**.

Examples

The following example connects to an openflow controller in active mode.

```
device# configure terminal
device(config)# openflow controller ip-address 10.2.3.4
device(config)# openflow controller ip-address 10.2.3.4 no-ssl port 6635
```

The following example connects to an openflow controller in passive mode.

```
device# configure terminal
device(config)# openflow controller passive no-ssl
device(config)# openflow controller passive no-ssl ip-address 10.2.3.6
```

NOTE

Passive mode connections are intended for testing environments and not recommended for production environments.

History

Release	Command History
08.0.30	This command was introduced.

openflow default send-to-controller

Configures a device-level option to forward the packets to the controller.

Syntax

openflow default send-to-controller

no openflow default send-to-controller

Command Default

The **no openflow default send-to-controller** is not enabled.

Modes

Global configuration mode

Examples

The following example configures a device-level option to forward the packets to the controller.

```
device# configure terminal
device(config)# openflow default send-to-controller
```

History

Release	Command History
08.0.30	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**]]

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.

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 1.0 is enabled, the following example configures Layer 2 and Layer 3 matching mode for flows.

```
device# configure terminal
device(config)# openflow enable ofv100
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# openflow enable layer23 hybrid-mode
```

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
08.0.20	This command was introduced.
08.0.30	Added example for the openflow 1.0.

openflow hello-reply disable

Enables the second hello message sent from the switch to the controller.

Syntax

openflow hello-reply disable

no openflow hello-reply disable

Command Default

The second hello message is enabled.

Modes

Global configuration mode

Usage Guidelines

There are two hello messages sent from the switch to the controller during the connection establishment. Use the no openflow hello-reply disable command to disable the second hello message for unexpected interruption to the connection to the controller.

Examples

The following example disables the second hello message from the switch to the controller.

```
device# configure terminal
device(config)# no openflow hello-reply disable
```

History

Release	Command History
08.0.30	This command was introduced.

openflow log timeout

Enables or disables the syslog message that is generated when a flow is deleted as a result of idling or hard timeout.

Syntax

openflow log timeout

no openflow log timeout

Command Default

The openflow log timeout is enabled.

Modes

Global configuration mode

Examples

The following example enables the openflow log timeout syslog message.

```
device# configure terminal
device(config)# openflow log timeout
```

The following example disables the openflow log timeout syslog message.

```
device# configure terminal
device(config)# no openflow log timeout
```

History

Release	Command History
08.0.30	This command was introduced.

openflow protected-vlans

Enables or disables the protected VLANs on an OpenFlow hybrid port mode interface.

Syntax

openflow protected-vlans *vlan-id*

no protected-vlans *vlan-id*

Parameters

vlan-id

Specifies a VLAN.

Modes

Global configuration mode

Interface configuration mode

Examples

After OpenFlow 1.0 is enabled, the followig example add a protected VLANs on an OpenFlow hybrid port mode interface.

```
device# configure terminal
device(config)# openflow enable ofv100
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# openflow enable layer23 hybrid-mode
device(config-if-1/1/1)# openflow protected-vlans 400
```

After OpenFlow 1.3 is enabled, the followig example add a protected VLANs on an OpenFlow hybrid port mode interface.

```
device# configure terminal
device(config)# openflow enable ofv130
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# openflow enable layer23 hybrid-mode
device(config-if-1/1/1)# openflow protected-vlans 400
```

History

Release	Command History
08.0.30	This command was introduced.

openflow purge-time

Configures the maximum amount of time (in seconds) before stale flows are purged from the OpenFlow flow table after a switchover, failover, or OS upgrade.

Syntax

openflow purge-time seconds

no openflow purge-time seconds

Command Default

The value of the OpenFlow purge timer is the default value for normal circumstances.

Parameters

seconds

Specifies the maximum amount of time (in seconds), before stale flows are purged. The range is from 1 through 600. The default is 240 seconds.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

You can configure a larger value for the OpenFlow purge timer, if delay is anticipated in learning the flows from controller after switch-over.

Examples

The following example sets the OpenFlow purge time to 500 seconds:

```
device(config)# openflow purge-time 500
```

History

Release version	Command history
08.0.30	This command was introduced.

optical-monitor

Configures the device to monitor optical transceivers in the system, either globally or by specified ports.

Syntax

optical-monitor [*alarm-interval*]

no optical-monitor [*alarm-interval*]

Command Default

Optical monitoring is not enabled.

The default interval between which alarms and warning messages are sent in 3 minutes. The default interval for the ICX 6650 is 8 minutes.

Parameters

alarm-interval

Specifies the interval between which alarms and warning messages are sent. The value can range from 1 to 65535. For the ICX 6650 enter a value between 8 and 65535. Enter 0 to disable alarms and warning messages.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

You can configure your Brocade device to monitor optical transceivers in the system, either globally or by specified ports. When this feature is enabled, the system will monitor the temperature and signal power levels for the optical transceivers in the specified ports. Console messages and Syslog messages are sent when optical operating conditions fall below or rise above the XFP, SFP, and SFP+ manufacturer recommended thresholds.

A Brocade chassis device can monitor a maximum of 24 SFPs and 12 XFPs.

NOTE
A Brocade ICX 6650 device allows all ports to support Digital Optical Monitoring (DOM).

NOTE
The commands **no optical-monitor** and **optical-monitor 0** perform the same function. That is, they both disable digital optical monitoring.

The **no** form of the command to disable digital optical monitoring.

Examples

The following example shows how to enable optical monitoring on all Brocade-qualified optics installed in the device.

```
device(config)# optical-monitor
```

The following example shows how to enable optical monitoring on a specific port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# optical-monitor
```

The following example shows how to set the interval to 10 minutes.

```
device(config)# interface ethernet 1/1/1 to 1/1/4
device(config-mif-e10000-1/1/1-1/1/4)# optical-monitor 10
```

option

Specifies the vendor-specific information (VSI) to be exchanged between the server and the client (option 43).

Syntax

option { **ascii** | **hex** } *ASCII string*

Parameters

ascii

Specifies the comma-separated ASCII value of the vendor-specific information.

hex

Specifies the hexadecimal value of the vendor-specific information.

ASCII string

The value of the vendor-specific information.

Modes

DHCP server pool configuration mode

Usage Guidelines

DHCP Option 43 can contain any vendor-specific information. The DHCP server passes this information in the form of a hex string or an ASCII string to the clients that receive the DHCP ACK.

Configuring DHCP option 60 helps in identifying the incoming DHCP client. If the vendor class identifier advertised by the DHCP client matches with the DHCP server, the server makes a decision to exchange the vendor-specific information configured as part of DHCP option 43.

Examples

The following example configures option 43 using the ASCII option for a Ruckus AP.

```
device# configure terminal
device(config)# ip dhcp-server pool ruckus
device(ip dhcp-server pool ruckus)# option 43 ascii 192.168.10.1,192.168.20.01,192.168.30.1
device(ip dhcp-server pool ruckus)# deploy
```

The following example configures option 43 using the hex option for a Ruckus AP.

```
device# configure terminal
device(config)# ip dhcp-server pool ruckus
device(ip dhcp-server pool ruckus)# option 43 hex 0108c0a8a01cc0a81401
device(ip dhcp-server pool ruckus)# deploy
```

History

Release version	Command history
08.0.30mb	This command was introduced.

originator-id

Configures MSDP to use the specified interface IP address as the IP address of the rendezvous point (RP) in a source-active (SA) message.

Syntax

originator-id *type number*

no originator-id *type number*

Command Default

MSDP uses the IP address of the originating RP in the RP address field of the SA message.

Parameters

type

Specifies the type of interface used by the RP. You can use Ethernet, loopback, and virtual routing interfaces (ve).

number

Specifies the interface number. For example, the Ethernet port number, loopback number, or virtual routing interface number.

Modes

MSDP router configuration mode

MSDP router VRF configuration mode

Usage Guidelines

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

Examples

This example configures an interface IP address to be the IP address of the RP.

```
Device(config)# interface loopback 2
Device(config-lbif-2)# ip address 2.2.1.99/32
Device(config)# router msdp
Device(config-msdp-router)# originator-id loopback 2
Device(config-msdp-router)# exit
```

This example configures an interface IP address to be the IP address of the RP on a VRF named blue.

```
Device(config)# interface loopback 2
Device(config-lbif-2)# ip address 2.2.1.99/32
Device(config)# router msdp vrf blue
Device(config-msdp-router-vrf blue)# originator-id loopback 2
Device(config-msdp-router-vrf blue)# exit
```

other-proto

Configures the other protocol VLAN and enters the other protocol VLAN configuration mode.

Syntax

other-proto [**name** *string*]

no other-proto [**name** *string*]

Command Default

IP protocol VLANs are configured.

Parameters

name *string*

Specifies the name of the other protocol VLAN configuration. The name can be up to 32 characters in length.

Modes

VLAN configuration mode

IP protocol VLAN configuration mode

IPX protocol VLAN configuration mode

IPv6 protocol VLAN configuration mode

DECnet protocol VLAN configuration mode

NetBIOS protocol VLAN configuration mode

AppleTalk protocol VLAN configuration mode

Usage Guidelines

The **no** form of the command removes the other protocol VLANs.

Examples

The following example shows how to configure the other protocol VLAN.

```
device(config)# ipx-proto name Brown
device(config-vlan-ipx-proto)# other-proto name Block_other_proto
device(config-vlan-other-proto)# no dynamic
```

packet-inerror-detect

Enables the monitoring of a port for inError packets and defines the maximum number of inError packets allowed for the port during the configured sampling interval.

Syntax

packet-inerror-detect *inError-count*

no packet-inerror-detect *inError-count*

Command Default

The Packet InError Detect feature is disabled for the port.

Parameters

inError-count

Specifies the maximum number of inError packets that are allowed for a port during the configured sampling interval. The value can range from 10 through 4294967295.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command disable monitoring of inError packets for the port.

If the number of inError packets received at a port exceeds the default value for two consecutive sampling windows, the port is set to the error-disabled state.

NOTE
To enable monitoring of inError packets for the port only, you must first use the **errdisable packet-inerror-detect** command in global configuration mode to globally enable monitoring for inError packets on the device.

Examples

The following example displays the maximum number of allowed inError packets for a port set to the value 10.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# packet-inerror-detect 10
```

History

Release version	Command history
07.3.00g	This command was introduced.

pass-through

Enables pass-through which allows certain protocol packets to pass through ports that are enabled for Flexible authentication.

Syntax

pass-through { **cdp** | **fdp** | **lldp** }

no pass-through{ **cdp** | **fdp** | **lldp** }

Command Default

Pass-through is not enabled.

Parameters

cdp

Specifies the Cisco Discovery Protocol to pass through.

fdp

Specifies the Foundry Discovery Protocol to pass through.

lldp

Specifies the Link Layer Discovery Protocol to pass through.

Modes

Authentication mode

Usage Guidelines

This command specifies the protocols to be passed through even though the client is not authenticated.

The **no** form of the command disables pass-through.

Examples

The example enables LLDP for pass-through.

```
device(config)# authentication
device(config-authen)# pass-through lldp
```

History

Release version	Command history
08.0.20	This command was introduced.

peer

Configures the software clock to synchronize a peer or to be synchronized by a peer.

Syntax

peer { *ipv4-address* | *ipv6-address* } [**version** *version-number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**burst**]

no peer { *ipv4-address* | *ipv6-address* } [**version** *version-number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**burst**]

Command Default

Peer is not configured.

Parameters

ipv4-address
: Specifies the IPv4 address of the peer providing the clock synchronization.

ipv6-address
: Specifies the IPv6 address of the peer providing the clock synchronization.

version *version-number*
: Specifies the Network Time Protocol (NTP) version number. Valid values are 3 or 4. The default value is 4.

key *key-id*
: Specifies the authentication key. By default, no authentication key is configured. The value can range from 1 to 65535.

minpoll *interval*
: Specifies the shortest polling interval. The range is from 4 through 17. Default is 6. The interval argument is power of 2 (4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s, and so on).

maxpoll *interval*
: Specifies the longest polling interval. The range is from 4 through 17. Default is 10. The interval argument is calculated by the power of 2 (4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s, and so on).

burst
: Sends a burst of packets to the server at each polling interval.

Modes

NTP configuration mode

Usage Guidelines

NTP peer mode is intended for configurations where a group of devices operate as mutual backups for each other. If one of the devices loses a reference source, the time values flow from the surviving peers to all the others.

A maximum of 8 NTP peers can be configured.

NOTE
The **peer** command is not effective if the NTP is enabled in client-only mode.

NOTE
If the peer is a member of symmetric passive association, then configuring the **peer** command will fail.

The **no** form of the command disables the software clock to synchronize a peer.

Examples

The following example shows how to configure the software clock.

```
device(config)# ntp
device(config-ntp)# peer 2.2.2.2 key 23 maxpoll 15 minpoll 7 version 4 burst
```

peer disable-fast-failover

Disables the MCT fast-failover mode.

Syntax

peer *peer-ip* **disable-fast-failover**

no peer *peer-ip* **disable-fast-failover**

Command Default

Fast-failover is configured on the device.

Parameters

peer-ip

Specifies the IP address of the peer device.

Modes

Cluster configuration mode

Usage Guidelines

The following failover modes can be configured with MCT:

- Fast-failover (default) - As soon as the ICL interface goes down, the MCT control path between the two peer devices goes down. All the remote MAC addresses are flushed.
- Slow-failover - Even if the ICL interface goes down, the CCP waits for the hold-time before taking the MCT control path between the two peer devices down. Remote MAC addresses are flushed only when the MCT control path between the two peer devices is down.

The **no** form of the command re-enables fast-failover.

Examples

The following example shows how to disable fast-failover.

```
device(config)# cluster SX
device(config-cluster-SX)# peer 10.1.1.3 disable-fast-failover
```

peer rbridge-id

Configures the MCT cluster peer.

Syntax

peer *peer-ip* **rbridge-id** *peer-rbridge* **icl** *map-icl*

no peer*peer-ip* **rbridge-id** *peer-rbridge* **icl** *map-icl*

Command Default

MCT cluster peer information is not configured.

Parameters

peer-ip

Specifies the IP address of the peer device.

rbridge-id *peer-rbridge*

Specifies the cluster RBridge ID. The value can be from 1 through 4095.

icl *map-icl*

Specifies the mapped cluster ICL name. The name is an ASCII string up to 64 characters in length.

Modes

Cluster configuration mode

Usage Guidelines

Configuration of the peer device involves the peer's IP address, RBridge ID, and ICL specification. The RBridge ID must be different from the cluster RBridge ID and any other client in the cluster. The MCT member VLAN is defined as any VLAN of which the ICL is a member.

The **no** command removes the MCT cluster peer.

Examples

The following example shows how to configure cluster peer information.

```
device(config)# cluster SX 4000
device(config-cluster-SX)# rbridge-id 3
device(config-cluster-SX)# session-vlan 3000
device(config-cluster-SX)# keep-alive-vlan 3001
device(config-cluster-SX)# icl SX-MCT ethernet 1/1/7
device(config-cluster-SX)# peer 10.1.1.2 rbridge-id 2 icl SX-MCT
device(config-cluster-SX)# deploy
```

peer timers

Configures the keep-alive and hold-time timers for peer devices.

Syntax

peer *peer-ip* **timers keep-alive** *keep-alive-timer* **hold-time** *hold-timer*

no peer *peer-ip* **timers keep-alive** *keep-alive-timer* **hold-time** *hold-timer*

Command Default

The default value for the keep-alive timer is 10 seconds.

The default value for the hold-time timer is 90 seconds.

Parameters

peer-ip
Specifies the IP address of the cluster peer.

keep-alive *keep-alive-timer*
Specifies the keep-alive interval in seconds. The value can range from 0 through 21845 seconds.

hold-time *hold-timer*
Specifies the hold-time interval in seconds. The value can range from 3 through 65535 seconds (or 0 if the keep-alive timer is set to 0).

Modes

Cluster configuration mode

Usage Guidelines

The *peer-ip* parameter should be in the same subnet as the cluster management interface. The hold-time must be at least three times the keep-alive time.

NOTE
The keep-alive VLAN and keep-alive timers are not related. The keep-alive timer is used by CCP.

The **no** form of the command sets the timers to the default values.

Examples

The following example shows how to configure the peer timers.

```
device(config)# cluster SX 400
device(config-cluster-SX))# peer 10.1.1.3 timers keep-alive 40 hold-time 120
```

peer-info

Configures the peer system ID and system key for a single dynamic Link Aggregation Group (LAG).

Syntax

peer-info sys-mac *mac-address* **sys-pri** *number* **key** *key number*

no peer-info sys-mac *mac-address* **sys-pri** *number* **key** *key number*

Command Default

The peer information of any one of the ports of a dynamic LAG that forms the first LACP trunk within that dynamic LAG, is considered as the peer information.

Parameters

sys-mac *mac-address*

Specifies the system's peer Ethernet MAC address.

sys-pri *number*

Specifies the LACP system priority for the system's peer. Valid numbers range from 0 through 65535.

key *key number*

Specifies the LACP key value. Valid key numbers range from 1 through 65535.

Modes

LAG configuration mode

Usage Guidelines

The **no** form of the command removes the peer information configuration for the dynamic LAG.

Examples

The following example configures the peer system with a system priority of 10 and an LACP key value of 10000.

```
device(config)# lag R4-dyn2
device(config-lag-R4-dyn2)# peer-info sys-mac 0000.0000.0003 sys-pri 10 key 10000
```

History

Release version	Command history
8.0.30d	This command was introduced.

pdu-rate (EFM-OAM)

Configures the number of Protocol Data Units (PDUs) to be transmitted per second by the Data Terminal Equipment (DTE).

Syntax

pdu-rate *value*

no pdu-rate *value*

Command Default

The default value is one PDU per second.

Parameters

value

Specifies the number of PDUs to be sent per second. The value range can be from 1 through 10 PDUs per second.

Modes

EFM-OAM protocol configuration mode

Usage Guidelines

If the PDU rate is configured as 10 packets per second, PDUs may not get transmitted in a timely manner according to the configured PDU rate.

The **no** form of the command restores the default value of one PDU per second.

Examples

The following example configures the PDU rate as 6 PDUs per second.

```
device(config)# link-oam
device(config-link-oam)# pdu-rate 6
```

History

Release version	Command history
08.0.30	This command was introduced.

phy cable diagnostics tdr

Runs the VCT TDR test on the specified port.

Syntax

phy cable-diagnostics tdr*stackid/slot/port*

Parameters

stackid/slot/port

Specifies the interface (port), by device, slot, and port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear TDR test registers before every TDR cable diagnostic test.

Before executing this command, use the **clear cable-diagnostics tdr** command to clear any previous TDR test results.

Display diagnostic test results using the **show cable-diagnostics tdr stackid/slot/port** command.

This command is just supported for ICX 6xxx series devices.

Examples

The following example clears test registers for the interface and then runs the TDR diagnostic test for port 3 on slot 2 of the first device in the stack.

```
device# clear cable-diagnostics tdr 1/2/3
device# phy cable-diag tdr 1/2/3
```

History

Release version	Command history
08.0.20	This command was introduced for ICX 6610, ICX 6430, ICX 6430-C, ICX 6450, and ICX6450-C devices.

phy-fifo-depth

Configures the depth of the transmit and receive FIFOs.

Syntax

phy-fifo-depth *value*

no phy-fifo-depth *value*

Command Default

The default value is 0.

Parameters

value

Specifies the setting value. There are 4 settings (0-3) with 0 as the default.

Modes

Interface configuration mode

Usage Guidelines

PHY devices on Brocade devices contain transmit and receive synchronizing FIFOs to adjust for frequency differences between clocks. The **phy-fifo-depth** command allows you to configure the depth of the transmit and receive FIFOs. A higher setting indicates a deeper FIFO.

The default setting works for most connections. However, if the clock differences are greater than the default will handle, CRCs and errors will begin to appear on the ports. Raising the FIFO depth setting will adjust for clock differences.

It is recommend that you disable the port before applying this command, and re-enable the port. Applying the command while traffic is flowing through the port can cause CRC and other errors for any packets that are actually passing through the PHY while the command is being applied.

This command can be issued for a single port from the interface config mode or for multiple ports from the MIF config mode.

The **no** form of the command removes the depth of the transmit.

Examples

The following example shows how to configure the phy-fifo-depth for a single port.

```
device(config)# interface ethernet 1/1/21
device(config-if-e1000-1/1/21)# phy-fifo-depth 2
```

The following example shows how to configure the phy-fifo-depth for multiple ports.

```
device(config)# interface ethernet 1/1/1 to 1/1/5
device(config-mif-1/1/1-1/1/5)# phy-fifo-depth 1
```

ping

Verifies that a device can reach another device through the network.

Syntax

ping { *ip-addr* | *hostname* | **vrf** *vrf-name* | **ipv6** [*ipv6-addr* | *hostname* | **vrf** *vrf-name*] [**outgoing-interface** *type number*] } [**source** *ip-addr*] [**count** *num*] [**timeout** *msec*] [**ttl** *num*] [**size** *num*] [**quiet**] [**numeric**] [**no-fragment**] [**verify**] [**data** *1-to-4-byte-hex*] [**brief** [**max-print-per-sec** *number*]]

Parameters

ip-addr

Specifies the IP address of the device.

hostname

Specifies the host name of the device.

vrf *vrf-name*

Specifies the VRF instance of the device.

ipv6

Specifies the IPv6 address, hostname or VRF instance of the device.

outgoing-interface *type number*

Specifies an interface over which you can verify connectivity.

source *ip-addr*

Specifies an IP address to be used as the origin of the ping packets.

count *num*

Specifies the number of ping packets the device sends. The value can range from 1 to 4294967296. The default is 1.

timeout *msec*

Specifies the time the device waits for a reply from the pinged device. The value can range from 1 to 4294967296 milliseconds. The default is 5000 (5 seconds).

ttl *num*

Specifies the maximum number of hops. The value can range from 1 to 255. The default is 64.

size *byte*

Specifies the size of the ICMP data portion of the packet. This is the payload and does not include the header. The value can range from 0 to 10000. The default is 16.

no-fragment

Turns on the "don't fragment" bit in the IP header of the ping packet. This option is disabled by default.

quiet

Hides informational messages such as a summary of the ping parameters sent to the device and instead only displays messages indicating the success or failure of the ping. This option is disabled by default.

verify

Verifies that the data in the echo packet (the reply packet) is the same as the data in the echo request (the ping). By default the device does not verify the data.

data*1-to-4-byte-hex*
Specifies a data pattern for the payload instead of the default data pattern, "abcd", in the packet data payload. The pattern repeats itself throughout the ICMP message (payload) portion of the packet.

brief
Specifies that the ping test characters is to be displayed. For more information refer to the Usage Guidelines section.

max-print-per-sec *number*
Specifies the maximum number of target responses the device can display per second while in brief mode. The value can range from 0 to 2047. The default is 511.

Modes

All configuration modes

Usage Guidelines

The following ping test characters are supported:

- ! - Indicates that a reply was received.
- . - Indicates that the network server timed out while waiting for a reply.
- U - Indicates that a destination unreachable error PDU was received.
- I - Indicates that the user interrupted ping.

For numeric parameter values, the command does not check that the value you enter is within the allowed range. Instead, if you do exceed the range for a numeric value, the software rounds the value to the nearest valid value.

NOTE
If the device is a Layer 2 Switch or Layer 3 Switch, you can use the host name only if you have already enabled the Domain Name Server (DNS) resolver feature on the device from which you are sending the ping.

Examples

The following example shows how to check the connectivity of the device 10.33.4.7.

```
device> ping 10.33.4.7
```

port-name

Configures port names to individual ports or to a group of ports.

Syntax

port-name *text*

no port-name *text*

Command Default

Port name is not configured.

Parameters

text

Configures the name of the port. The name is an alphanumeric string and can be up to 255 characters long.

Modes

Interface configuration mode

Usage Guidelines

You can assign a port name to physical ports, virtual interfaces, and loopback interfaces. The port name can contain blanks. The port name can contain special characters as well, but the percentage character (%) is dropped if it is the last character in the port name.

The **no** form of the command removes the assigned port name.

Examples

The following example shows how to assign a name to a port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# port-name Marsha
```

The following example shows how to assign a name to a range of ports.

```
device(config)# interface ethernet 1/1/1 to 1/1/10
device(config-mif-1/1/1-1/1/10)# port-name connected-to-the nearest device
```

The following example shows how to assign a name to multiple specific ports.

```
device(config)# interface ethernet 1/1/1 ethernet 1/1/5 ethernet 1/1/7
device(config-mif-1/1/1,1/1/5,1/1/7)# port-name connected-to-the nearest device
```

port-name (LAG)

Assigns a port name to an individual port in a LAG.

Syntax

port-name *name* **ethernet** *stackid/slot/port*

no port-name *name* **ethernet** *stackid/slot/port*

Command Default

A port name is not assigned to an individual port within a LAG.

Parameters

name

Specifies the name of an individual port in a LAG. The name can be up to 255 characters in length.

ethernet *stackid/slot/port*

Specifies the Ethernet port to which the name must be assigned.

Modes

LAG configuration mode

Usage Guidelines

When creating a port name in a LAG, you can use all uppercase or lowercase characters, as well as digits. Special characters (such as $, %, ', -, ., @, ~, `, !, (,), {, }, ^, #, and &) are valid. You can use spaces in the port name as long as you enclose the name in double quotation marks. For example, to specify a port name that contains spaces, enter a string similar to the following example: "a long and lengthy port name".

NOTE

A port name with spaces must be enclosed within double quotation marks.

The **no** form of the command removes the name assigned to the individual port.

Examples

The following example shows how to assign a name to a port in a LAG.

```
device(config)# lag "test" dynamic id 1
device(config-lag-test)# ports ethernet 1/1/1 to 1/1/3
device(config-lag-test)# port-name "Brocade lag" ethernet 1/1/1
device(config-lag-test)# primary-port 1/1/1
device(config-lag-test)# deploy
```

port security

Enters port security configuration mode.

Syntax

port security

Modes

Global configuration mode

Usage Guidelines

Use the **enable** command to enable port security.

Examples

The following example shows how to enter port security configuration mode.

```
device(config)# port security
device(config-port-security)#
```

port-down-authenticated-mac-cleanup

Enables forced reauthentication of the hosts if all the ports on the device go down.

Syntax

port-down-authenticated-mac-cleanup

no port-down-authenticated-mac-cleanup

Command Default

Forced reauthentication of hosts is enabled.

Modes

Web Authentication configuration mode

Usage Guidelines

When the command is enabled, the device checks the link state of all ports that are members of the Web Authentication VLAN. If the state of all the ports is down, then the device forces all authenticated hosts to reauthenticate. However, hosts that were authenticated using the **add mac** command will remain authenticated; they are not affected by the **port-down-authenticated-mac-cleanup** command.

The **no** form of the command removes forced reauthentication of the hosts.

Examples

The following example enables forced reauthentication of all hosts when all the ports are down.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# port-down-authenticated-mac-cleanup
```

port-down-disable-laser

Enables you to switch off the laser light emission, when a port is disabled.

Syntax

port-down-disable-laser

no port-down-disable-laser

Command Default

If the CLI configuration is present, the laser is switched off automatically when the port is disabled.

Modes

Ethernet interface configuration mode.

Usage Guidelines

The CLI is supported only on 1G SFP and 10G SFP+ fiber ports. It is not supported on copper ports and CGBIC. Also, this is not supported on ICX6610, ICX6450, ICX6430, ICX7750, SXL, ICX 6650 and on 40G ports.

The command is present in the running configuration and is applicable per port at the interface level. The command persist across reloads. Laser is switched on or off based on the CLI configuration and the port status (enable or disable). If the CLI configuration is present, the laser is switched off automatically when the port is disabled. You can apply the CLI configuration irrespective of the port state (enable or disable).

If the **port-down-disable-laser** command is configured on the port, the laser emission is switched off when the port is disabled. However, if the command is removed from the disabled port, turning on the laser light must be taken care manually when the port is enabled. The command does not support global configuration.

Examples

```
device(config-if-e1000-1/1/1)# port-down-disable-laser
device(config-if-e1000-1/1/1)# disable
```

History

Release version	Command history
8.0.30n	This command was introduced.

ports

Adds ports in a LAG.

Syntax

ports ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no ports ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

No ports are added to the LAG.

Parameters

ethernet *stackid/slot/port*
Adds an Ethernet interface to a LAG.

to *stackid/slot/port*
Adds a range of Ethernet interfaces to the LAG.

Modes

LAG configuration mode

Usage Guidelines

A static or dynamic LAG can have 1 to 8 or 1 to 12 ports (depending on the device you are using) of the same type and speed that are on any interface module within the Brocade chassis. A keep-alive LAG consists of only one port.

Ports can be added to an undeployed LAG or to a currently deployed LAG. When deleting ports from a currently deployed LAG, the primary port cannot be removed. If removal of a port will result in the trunk threshold value becoming greater than the number of ports in the LAG, the port deletion will be rejected. When you remove a port from a deployed LAG, the port is disabled automatically.

NOTE
When a port is deleted from a currently deployed LAG, the MAC address of the port is changed back to its original value.

NOTE
In an operational dynamic LAG, removing an operational port causes port flapping for all LAG ports. This may cause loss of traffic.

The **no** form of the command removes the ports from a LAG.

Examples

The following example shows how to configure a static LAG with two ports.

```
device(config)# lag blue static
device(config-lag-blue)# ports ethernet 1/3/1 ethernet 1/3/2
```

The following example adds a range of ports to the LAG.

```
device(config)# lag blue static
device(config-lag-blue)# ports ethernet 1/3/1 to 1/3/4
```

The following example adds a range of ports from one interface module and an individual port from another interface module to the LAG.

```
device(config)# lag blue static
device(config-lag-blue)# ports ethernet 1/3/1 to 1/3/4 ethernet 1/2/2
```

port-statistics-reset-timestamp enable

Enables the display of the elapsed timestamp information in the output of the **show statistics** command.

Syntax

port-statistics-reset-timestamp enable

no port-statistics-reset-timestamp enable

Command Default

The elapsed time after the recent reset of the port statistics counters is not displayed in the **show statistics** command output.

Modes

Global configuration mode

Usage Guidelines

The elapsed time is calculated as the time between the most recent reset of the port statistics counters and the time when the **show statistics** command is executed.

The **port-statistics-reset-timestamp enable** command enables the display of the elapsed timestamp information for all the ports in the output of the **show statistics** command.

The **no** form of the command removes the display of the elapsed time after the most recent reset of the port statistics counters in the **show statistics** command output.

Examples

The following example enables the display of the elapsed time between the most recent reset of the port statistics counters and the time when the **show statistics** command is executed.

```
device (config)# port-statistics-reset-timestamp enable
```

History

Release version	Command history
08.0.30	This command was introduced.

prefix-list

Associates an IPv6 prefix list with a Router Advertisement (RA) guard policy.

Syntax

prefix-list *name*

no prefix-list *name*

Parameters

name

Specifies the name of the IPv6 prefix list to associate with the RA guard policy.

Modes

RA guard policy configuration mode

Usage Guidelines

This command associates an IPv6 prefix list with an RA guard policy so that only the RAs that have the given prefix are forwarded. You must provide the name of an IPv6 prefix list already configured using the **ipv6 prefix-list** command. For more information on configuring an IPv6 prefix list using the **ipv6 prefix-list** command, see the *FastIron Ethernet Switch Layer 3 Routing Configuration Guide* .

Only one prefix list can be associated with an RA guard policy. If the command is configured twice with different prefix lists, the latest configured prefix list is associated with the RA guard policy.

no

Examples

The following example associates an IPv6 prefix list with an RA guard policy:

```
Brocade(config)# ipv6 prefix-list raguard-prefix1
Brocade(config)# ipv6 raguard policy p1
Brocade(config-ipv6-RAG-policy p1)# prefix-list raguard-prefix1
```

preforwarding-time

Configures the preforwarding time interval, the time a port will remain in the preforwaring 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 500 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
```

pre-shared-key

Configures the pre-shared MACsec key on the interface.

Syntax

pre-shared-key *key-id* **key-name** *hex-string*

no pre-shared-key *key-id* **key-name** *hex-string*

Command Default

No pre-shared MACsec key is configured on the interface.

Parameters

key-id

Specifies the 32 hexadecimal value used as the Connectivity Association Key (CAK).

key-name *hex-string*

Specifies the name for the CAK key. Use from 2 through 64 hexadecimal characters to define the key name.

Modes

dot1x-mka interface mode

Usage Guidelines

The **no** form of the command removes the pre-shared key from the interface.

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

The pre-shared key is required for communications between MACsec peers.

Examples

The following example configures MKA group test1 and assigns the MACsec pre-shared key with a name beginning with 96437a93 and with the value shown, to port 2, slot 3 on the first device in the stack.

```
device(config)#dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group test1
device(config-dot1x-mka-group-test1)# key-server-priority 5
device(config-dot1x-mka-group-test1)# macsec cipher-suite gcm-aes-128
device(config-dot1x-mka-group-test1)# macsec confidentiality-offset 30
device(config-dot1x-mka-group-test1)# exit
device(config-dot1x-mka)# enable-mka ethernet 1/3/2
device(config-dot1x-mka-1/3/2)# mka-group test1
device(config-dot1x-mka-1/3/2)# pre-shared-key 135bd758b0ee5c11c55ff6ab19fdb199 key-name
96437a93ccf10d9dfe347846cce52c7d
```

History

Release version	Command history
08.0.20	This command was introduced.

primary-port

Configures the primary port in a LAG.

Syntax

primary-port *stackid/slot/port*

no primary-port *stackid/slot/port*

Command Default

The primary-port is not configured.

Parameters

stackid/slot/port

Designates the primary port in a LAG.

Modes

LAG configuration mode

Usage Guidelines

Once a primary port has been configured for a LAG, all configurations that apply to the primary port are applied to the other ports in the LAG.

NOTE
The primary port configuration is only applicable for static or dynamic LAGs.

The **no** form of the command removes the primary port.

Examples

The following example shows how to designate a primary port.

```
device(config)# lag blue static
device(config-lag-blue)# primary-port 1/1/2
```

priority

Configures a priority value for the device. This value is used along with other factors to determine controller election if a stack failover or merge occurs.

Syntax

priority *num*

no priority

Command Default

The priority value for the active controller and standby device is 128.

Parameters

num

Possible values are 0 to 255. Lower values assign a lower priority to the device, and higher values assign a higher priority to the device.

Modes

Stack unit configuration mode

Usage Guidelines

The **no** form of the command restores the default priority value to the device (128). You do not have to specify the default value when using the **no** form.

A unit that has a relatively high priority value is more likely to be elected to be the active controller.

When you change the priority value assigned to a stack unit, the value takes effect immediately but does not affect the active controller until the next reset.

When the active and standby controller have the same priority value, other factors affect controller election, such as up-time and number of members controlled.

Examples

The following example assigns a priority value of 130 to stack unit 1.

```
device(Config)# stack unit 1
device(Config-unit-1)# priority 130
```

History

Release version	Command history
08.0.01	This command was introduced.

priority-flow-control

Enables priority flow control (PFC) on a priority group.

Syntax

priority-flow-control *priority-group-number*

no priority-flow-control *priority-group-number*

Command Default

PFC is globally disabled

Parameters

priority-group-number

Specifies a priority group. The range is 0-3.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default flow-control settings.

To enable global PFC, symmetrical-flow-control must be disabled.

You must enable PFC globally before you configure it for priority groups.

Enabling PFC on a priority group enables PFC on all the ports.

PFC and 802.3x flow control are mutually exclusive. Configuring the **priority-flow-control** command disables 802.3x in both transmit and receive directions.

PFC is not supported for ports across stack units on ICX 7750 devices.

PFC is not supported on ICX 7450 devices.

Examples

The following example enables PFC for a priority group:

```
Device(config)# priority-flow-control enable
Device(config)# priority-flow-control 2
```

History

Release version	Command history
8.0.10	This command was introduced.

Release version	Command history
8.0.20	This command was modified. Specifying a priority group no longer enables PFC on all ports.

priority-flow-control enable

Enables priority flow control (PFC) globally or on an individual port.

Syntax

priority-flow-control enable

no priority-flow-control enable

Command Default

PFC is disabled (globally and on all ports).

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

In global configuration mode, the **no** form of this command restores the default flow-control settings. In interface configuration mode, the **no** form of the command disables PFC on the interface.

To enable global PFC, symmetrical-flow-control must be disabled.

You must enable PFC globally before you configure it for priority groups.

In global configuration mode, configuring the **priority-flow-control enable** command enables PFC globally; in interface configuration mode, configuring it enables PFC on a port. You can configure the **priority-flow-control enable** command in interface configuration mode to enable both PFC transmit and receive, that means PFC is both honored and generated. PFC must be enabled on at least one priority group before you can configure the **priority-flow-control enable** command on an interface.

Priority flow control and 802.3x flow control are mutually exclusive; therefore, configuring the **priority-flow-control enable** command disables 802.3x in both transmit and receive directions.

Examples

The following example enables PFC globally.

```
Device(config)# priority-flow-control enable
```

The following example enables PFC on an interface.

```
Device(config-if-e10000-1/1/1)# priority-flow-control enable
```

History

Release version	Command history
8.0.10	This command was introduced.

Release version	Command history
8.0.20	This command was modified to add enabling PFC on a port.

priority ignore-8021p

Enables 802.1p priority override.

Syntax

priority ignore-8021p

no priority ignore-8021p

Command Default

802.1p priority override is not enabled.

Modes

Interface configuration mode

Usage Guidelines

The command is not supported on FastIron ICX 7000 series devices.

You can configure a port to ignore the 802.1p priority for traffic classification for an incoming packet. When this feature is enabled, packets are classified as follows:

- If the packet matches an ACL that defines the priority, the ACL priority is used.
- If the packet source or destination MAC address matches a configured static MAC address with priority, the static MAC priority is used.
- If the ingress port has a configured priority, the port priority is used.
- If the above mentioned situations do not apply, the configured or default port priority (0) is used.

802.1p priority override is supported on physical ports.

802.1p is not supported with the **trust dscp** command.

The **no** form of the command disables 802.1p priority override.

Examples

The following example enables 802.1p priority override.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# priority ignore-8021p
```

privilege

Configures the management privilege access level of a command.

Syntax

privilege *command-mode* **level** *privilege-level command-string*

no privilege *command-mode* **level** *privilege-level command-string*

Parameters

command-mode

Specifies the command mode of the command for which you are enhancing the privilege access level.
Enter **?** to see which interface subtypes are available.

level *privilege-level*

Specifies the number of the management privilege level you are augmenting.
Valid values are 0 for Super User level (full read-write access), 4 for Port Configuration level, and 5 for Read Only level.

command-string

Specifies the command you want to allow with the specified privilege level to enter.
Enter **?** at the command prompt of a CLI level to display the list of commands at that level.

Modes

Global configuration mode.

Usage Guidelines

Each management privilege level provides access to specific areas of the CLI by default. You can grant additional access to a privilege level on an individual command basis. To grant the additional access, you specify the privilege level you are enhancing, the CLI level that contains the command, and the individual command.

Super User management privilege level provides access to all commands and displays. Port Configuration management privilege level gives access to the User EXEC level, Privileged EXEC level, the port-specific parts of the CONFIG level, and all interface configuration levels. Read Only management privilege level gives access to the User EXEC and Privileged EXEC levels.

NOTE
This command applies only to management privilege levels on the CLI.

The **no** form of the command removes the configurations and resets to default.

Examples

The following example shows how to enhance the Port Configuration privilege level so users also can enter IP commands at the global CONFIG level.

All users with Port Configuration privileges will have the enhanced access. Executing this command will enable users who log in with valid Port Configuration level user names and passwords to execute commands that start with "ip" at the global configuration level.

```
device(config)# privilege configure 4 ip
```

profile-config

Configures the port buffer, queue buffer, port descriptor, and queue descriptor for a port.

Syntax

profile-config { **port-buffers** *buffer-number* | **port-descriptors** *descriptor-number* | **port-type** { **0** | **1** | **2** | **3** } | **queue-buffers** *egress-queue-number buffer-number* | **queue-descriptors** *egress-queue-number descriptor-number* }

no profile-config { **port-buffers** *buffer-number* | **port-descriptors** *descriptor-number* | **port-type** { **0** | **1** | **2** | **3** } | **queue-buffers** *egress-queue-number buffer-number* | **queue-descriptors** *egress-queue-number descriptor-number* }

Command Default

The default port type is set to 1 Gbps.

The default buffers and descriptors are set according to the port type.

Parameters

port-buffers *buffer-number*
Configures the maximum buffer limit for the port.

port-descriptors *descriptor-number*
Configures the maximum descriptor limit for the port.

port-type
The port type for the user-configurable buffer profile.

0
Specifies the port type as 1 Gbps, 10 Gbps, or 40 Gbps.

1
Specifies the port type as 1 Gbps.

2
Specifies the port type as 10 Gpbs.

3
Specifies the port type as 40 Gbps.

queue-buffers
Configures the maximum buffer limit for the queues.

egress-queue-number
Specifies the egress queue number (0 through 7).

buffer-number
Specifies the buffer number.

queue-descriptors
Configures the maximum descriptor limit for the queues.

descriptor-number
Specifies the descriptor number.

Modes

Buffer profile configuration mode

Usage Guidelines

To configure a user-configurable profile for 10 Gbps ports, the 10 Gbps port type must be explicitly provided by the **port-type** option. Modifications to buffers and descriptors of a port and its queues take effect dynamically.

When the profile type is configured as all 1 Gbps, 10 Gbps, and 40 Gbps ports, the default buffers and descriptors will be set according to the port type; that is, all 1 Gbps ports use 1 Gbps defaults and 10 Gbps ports use 10 Gbps defaults. If you configure a port and its queue with egress buffer and descriptor limits, then the configured limits are used for both 1 Gbps and 10 Gbps ports.

Port type modification resets the profile to its default value. All the port and queue buffers and descriptors will be set to either 1 Gbps or 10 Gbps defaults as per the configuration, which means all the user configurations for the port and its queues will be lost.

NOTE
Port type modifications on an active profile are not allowed.

The **no** form of the command with the **port-type** option sets the profile port type to 1 Gbps.

Examples

The following example sets the port type to 10 Gbps.

```
device(config)# qd-buffer-profile 1
device(qd-profile-1)# profile-config port-type 3
```

The following example configures the port buffers.

```
device(config)# qd-buffer-profile 1
device(qd-profile-profile1)# profile-config port-buffers 8000
```

The following example configures the port descriptors.

```
device(config)# qd-buffer-profile 1
device(qd-profile-profile1)# profile-config port-descriptors 8000
```

The following example configures the queue buffer.

```
device(config)# qd-buffer-profile 1
device(qd-profile-profile1)# profile-config queue-buffers 2 600
```

The following example configures the queue descriptors.

```
device(config)# qd-buffer-profile 1
device(qd-profile-profile1)# profile-config queue-descriptors 2 600
```

protected-link-group

Configures a protected link group.

Syntax

protected-link-group *group-ID* [**active-port** *stackid/slot/port* | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]]

no protected-link-group *group-ID* [**active-port** *stackid/slot/port* | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]]

Command Default

A protected link group is not configured.

Parameters

group-ID
Specifies the protected link group number. The valid values are from 1 through 32.

active-port *stackid/slot/port*
Specifies the preferred active port to preempt other ports.

ethernet *stackid/slot/port*
Specifies the member Ethernet port.

to *stackid/slot/port*
Specifies a range of member ports to be added.

Modes

Global configuration mode

Usage Guidelines

NOTE
The command is not supported on ICX 7000 series devices.

There is no restriction on the number of ports in a protected link group. Each port can belong to one protected link group at a time.

You can use UDLD with protected link groups to detect unidirectional link failures and to improve the speed at which the device detects a failure in the link.

When two switches are connected together with links in a protected link group, and the ports connecting the switches together are part of a protected link group, you must configure two connecting ports (one port on each switch) as active ports of the protected link group.

If you do not explicitly configure an active port, the Brocade device automatically assigns one as the first port in the protected link group to come up.

NOTE
When UDLD and protected links are configured on a port and the link goes down, protected links will not come up after UDLD becomes "healthy" again without first physically disabling and then re-enabling the link.

The **no** form of the command removes the protected link group.

Examples

The following example shows how to configure a protected link group and its member ports.

```
device(config)# protected-link-group 10 ethernet 1/1/1 to 1/1/4
```

The following example shows how to assign an active port to a protected link group.

```
device(config)# protected-link-group 10 active-port 1/2/1
```

prune-timer

Configures the time a PIM device maintains a prune state for a forwarding entry.

Syntax

prune-timer *seconds*

no prune-timer *seconds*

Command Default

The prune time is 180 seconds.

Parameters

seconds

Specifies the interval in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the default prune time, 180 seconds.

The first received multicast interface is forwarded to all other PIM interfaces on the device. If there is no presence of groups on that interface, the leaf node sends a prune message upstream and stores a prune state. This prune state travels up the tree and installs a prune state. A prune state is maintained until the prune timer expires or a graft message is received for the forwarding entry.

Examples

This example configures a PIM prune timer to 90 seconds.

```
Device(config)# router pim
Device(config-pim-router)# prune-timer 90
```

prune-wait

Configures the time a PIM device waits before stopping traffic to neighbor devices that do not want the traffic.

Syntax

prune-wait *seconds*

no prune-wait

Command Default

The prune wait time is 3 seconds.

Parameters

seconds

Specifies the wait time in seconds. The range is 0 through 30 seconds. The default is 3 seconds.

Modes

PIM router configuration mode

Usage Guidelines

A smaller prune wait value reduces flooding of unwanted traffic. A prune wait value of 0 causes the PIM device to stop traffic immediately upon receiving a prune message.

If there are two or more neighbors on the physical port, you should not configure the **prune-wait** command because one neighbor may send a prune message while the other sends a join message at the same time, or within less than 3 seconds.

The **no** form of this command restores the default prune wait time of 3 seconds.

Examples

This example configures the prune wait time to 0 seconds.

```
device(config)# router pim
device(config-pim-router)# prune-wait 0
```

pvlan mapping

Identifies the other PVLANs for which the VLAN is the primary.

Syntax

pvlan mapping *vlan-id* **ethernet** *stackid/slot/port*

no pvlan mapping *vlan-id* **ethernet** *stackid/slot/port*

Command Default

PVLAN mapping is not configured.

Parameters

vlan-id

Specifies the other configured PVLAN.

ethernet *stackid/slot/port*

Specifies the primary VLAN port to which you are mapping all the ports in the other PVLAN (the one specified by *vlan-id*).

Modes

VLAN configuration mode

Usage Guidelines

The command also specifies the primary VLAN ports to which you are mapping the other secondary VLANs. A primary VLAN can have multiple ports. All these ports are active, but the ports that will be used depends on the PVLAN mappings. Also, secondary VLANs (isolated and community VLANs) can be mapped to one primary VLAN port.

The **no** form of the command disables the PVLAN mapping.

Examples

The following example shows how to configure PVLAN mapping.

```
device(config)# vlan 7
device(config-vlan-7)# untagged ethernet 1/3/2
device(config-vlan-7)# pvlan type primary
device(config-vlan-7)# pvlan mapping 901 ethernet 1/3/2
```

pvlan pvlan-trunk

Identifies the inter-switch link for the PVLAN.

Syntax

pvlan pvlan-trunk *num* **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]

no pvlan pvlan-trunk *num* **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]

Command Default

The inter-switch link for the primary VLAN is not configured.

Parameters

num

Specifies the VLAN ID.

ethernet *stackid/slot/port*

Configures the specified Ethernet port as the inter-switch link.

to *stackid/slot/port*

Configures a range of specified Ethernet ports as the inter-switch links.

Modes

VLAN configuration mode

Usage Guidelines

As with regular VLANs, PVLANs can span multiple switches. The PVLAN is treated like any other VLAN by the PVLAN-trunk ports. The PVLAN-trunk port is added to both the primary and the secondary VLANs as a tagged member through the **pvlan-trunk** command.

The **no** command deletes the inter-switch link for the primary VLAN.

Examples

The following example shows how to identify inter-switch link in the PVLAN.

```
device(config)# vlan 100
device(config-vlan-100)# tagged ethernet 1/1/10 to 1/1/11
device(config-vlan-100)# untagged ethernet 1/1/4
device(config-vlan-100)# pvlan type primary
device(config-vlan-100)# pvlan mapping 101 ethernet 1/1/4
device(config-vlan-100)# pvlan mapping 102 ethernet 1/1/4
device(config-vlan-100)# pvlan pvlan-trunk 101 ethernet 1/1/10 to 1/1/11
```

pvlan type

Configures the PVLAN as a primary, isolated, or community PVLAN.

Syntax

pvlan type { **community** | **isolated** | **primary** }

no pvlan type { **community** | **isolated** | **primary** }

Command Default

The PVLAN type is not configured.

Parameters

community
Creates a community PVLAN.

isolated
Creates an isolated PVLAN.

primary
Creates a primary PVLAN.

Modes

VLAN configuration mode

Usage Guidelines

The command configures the following PVLAN types:

- Community - Broadcasts and unknown unicasts received on community ports are sent to the primary port and also are flooded to the other ports in the community VLAN.
- Isolated - Broadcasts and unknown unicasts received on isolated ports are sent only to the primary port. They are not flooded to other ports in the isolated VLAN
- Primary - The primary PVLAN ports are "promiscuous". They can communicate with all the isolated PVLAN ports and community PVLAN ports in the isolated and community VLANs that are mapped to the promiscuous port.

For the primary VLAN, map the other PVLANs to the ports in the primary VLAN. VLAN identifiers configured as part of a PVLAN (primary, isolated, or community) should be consistent across the switched network. The same VLAN identifiers cannot be configured as a normal VLAN or a part of any other PVLAN. Member ports of isolated and community VLANs cannot be member ports of any other VLAN

LAG ports are not allowed as member ports of an isolated VLAN or community VLAN.

The **no** form of the command disables the PVLAN type.

Examples

The following example shows how to configure the community PVLAN.

```
device(config)# vlan 901
device(config-vlan-901)# untagged ethernet 1/3/5 to 1/3/6
device(config-vlan-901)# pvlan type community
```

The following example shows how to configure a primary PVLAN.

```
device(config)# vlan 7
device(config-vlan-7)# untagged ethernet 1/3/2
device(config-vlan-7)# pvlan type primary
```

pvst-mode

Enable PVST+ support on a port immediately.

Syntax

pvst-mode

no pvst-mode

Command Default

PVST+ support is automatically enabled when the port receives a PVST BPDU.

Modes

Interface configuration mode

Usage Guidelines

This command cannot be executed concurrently with the **pvstplus-protect** command.

If you disable PVST+ support, the software still automatically enables PVST+ support if the port receives a BPDU with the PVST+ format.

The **no** form of the command disables the PVST+ support.

Examples

The following example shows how to enable the PVST+ mode.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# pvst-mode
```

History

Release version	Command history
08.0.30mb	The Usage Guidelines were modified.

pvstplus-protect

Prevents flooding and resulting port blocking on an interface when a PVST+ packet is received on a port configured for MSTP, blocking the PVST+ BPDU and marking the port as ERR-DISABLED.

Syntax

pvstplus-protect

no pvstplus-protect

Command Default

This feature is disabled.

Modes

Interface configuration mode

Usage Guidelines

This command cannot be executed concurrently with the **pvst-mode** command.

When you execute the **pvstplus-protect** command, you must also execute the global **errdisable recovery pvstplus-protect** command to enable ports to recovery from the error-disabled state.

The **no** form of this command disables PVST+ Protect.

Examples

The following example enables PVST+ Protect on a single port.

```
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# pvstplus-protect
```

The following example confirms the configuration.

```
device(config)# show running-config interface ethernet 1/1/1
interface ethernet 1/1/1
 port-name ToCisco1
 dual-mode
 pvstplus-protect
```

The following example enables PVST+ Protect on a range of ports.

```
device(config)# interface ethernet 1/1/1 to 1/1/4
device(config-mif-1/1/1-1/1/4)# pvstplus-protect
```

NOTE

History

Release version	Command history
8.0.30mb	This command was introduced.

qd

Configures the queue depth limit for a port.

Syntax

qd *slot/port* { *depth-limit traffic-class* | **profile-id** *buffer-profile-id* }

no qd *slot/port* { *depth-limit traffic-class* | **profile-id** *buffer-profile-id* }

Command Default

The default for the queue depth limit is 4095.

Parameters

slot/port
: Specifies the slot and port number to set the queue depth limit.

depth-limit
: Configures the transmit queue depth limit for the port.

traffic-class
: Specifies the traffic class priority for the port. The traffic class ranges from 0 through 7, where 7 is the highest priority.

profile-id
: Configures the buffer profile ID of the port, if the port is associated with a buffer profile. The valid valuesare from 1 through 7.

buffer-profile-id
: Specifies the limit for the port. The valid values are from 0 through 4095.

Modes

Global configuration mode

Usage Guidelines

NOTE
The **qd** command is supported only on FSX devices.

The sum of the queue depth limits for individual traffic classes on a port do not need to equal the total queue depth limit for the port.

If the sum of the individual traffic class queue depth limits exceeds the total port limit and the total port limit is reached, any buffer that gets released can be used by any traffic class queue that has not reached its individual limit.

If the sum of the individual traffic class queue depth limits is less than the total port limit, the remaining buffers can be used only by packets with a priority of 7.

The **no** form of the command sets the default queue depth limit (4095) on the port.

Examples

The following example configures the transmit queue depth limit to 1000 on port 1/1.

```
device(config)# qd 1/1 1000
```

The following example configures the profile ID to 2 on port 1/1.

```
device(config)# qd 1/1 profile-id 2
```

qd-buffer

Configures the port buffers.

Syntax

qd-buffer *devicenum buffer-profile queue-depth* [*priorityqueue*]

no qd-buffer *devicenum buffer-profile quue-depth* [*priorityqueue*]

Command Default

Port buffers are not configured.

Parameters

devicenum

Specifies the device in the stacking unit. The device number starts from 1.

buffer-profile

Specifies the buffer profile. 1 for 1 Gbps ports, 2 for 10 Gbps ports and 3 for VoIP ports.

queue-depth

Specifies the number of buffers to allocate.

priorityqueue

Specifies the queue of the port from 0 through 7.

Modes

Global configuration mode

Usage Guidelines

The minimum limit for port buffers is 16. The maximum limit for the port buffer depends on the hardware device.

The **no** form of the command deletes the port buffers.

Examples

The following example shows how to configure the port buffers.

```
device(config)# qd-buffer 1 2 76
```

The following example shows how to configure the queue buffers.

```
device(config)# qd-buffer 1 2 76 2
```

qd-buffer-profile

Creates a user-configurable buffer profile for Quality of Service (QoS).

Syntax

qd-buffer-profile *profile-name*

no qd-buffer-profile *profile-name*

Command Default

A buffer profile is not created.

Parameters

profile-name

Specifies the user-defined buffer profile. The profile name can be up to 64 characters in length.

Modes

Global configuration mode

Usage Guidelines

Users can define a limit for a port and its queues by configuring the buffer profiles on the device. User-configurable buffer profiles provide a template to allocate egress buffers and descriptors limits to the port and on its queues. This template is then applied to the device.

Buffer profiles can be configured for 1 Gbps and 10 Gbps ports, but not for 40 Gbps ports on the Brocade ICX 6610. The 10 Gbps profile applies to ICX 6430 and ICX 6450 stacking ports, as well as FCX 16 Gbps stacking ports.

The no form of the command removes the buffer profile for QoS.

Examples

The following example creates the user-defined buffer profile for "profile1".

```
device(config)# qd-buffer-profile profile1
```

qd-descriptor

Configures the allowable port descriptors.

Syntax

qd-descriptor *devicenum buffer-profile numdescriptors* [*priorityqueue*]

no qd-descriptor *devicenum buffer-profile numdescriptors* [*priorityqueue*]

Command Default

Port descriptors are not configured.

Parameters

devicenum
: Specifies the device in the stacking unit. The device number starts from 0.

buffer-profile
: Specifies the buffer profile. 1 for 1 Gbps ports and 2 for 10 Gbps ports.

numdescriptors
: Specifies the number of descriptors to allocate.

priorityqueue
: Specifies the queue of the port from 0 through 7.

Modes

Global configuration mode

Usage Guidelines

Port descriptors set the limit for the ports. The minimum limit for port descriptors is 16. The maximum limit of the port descriptors depends on the hardware device. The minimum limit for queue descriptors is 16. The system default queue descriptors for different platforms are different.

The **no** form of the command deletes the port descriptors.

Examples

The following example shows how to configure the port descriptors.

```
device(config)# qd-descriptor 1 2 76
```

The following example shows how to configure the queue descriptors.

```
device(config)# qd-descriptor 1 2 76 2
```

qd-share-level

Configures the buffer sharing level for the device.

Syntax

qd-share-level *number*

no qd-share-level *number*

Command Default

The default buffer sharing level is 250 KB.

Parameters

number

The buffer sharing level for the device. The range of valid values for FCX, ICX 6450, and ICX 6430 devices is from 1 through 8. The range of valid values for an ICX 6610 is from 2 through 8. The levels represent the buffer sharing limit as 1 for 64 KB, 2 for 250 KB, 3 for 375 KB, 4 for 500 KB, 5 for 625 KB, 6 for 750 KB, 7 for 875 KB, and 8 for 1000 KB .

Modes

Global configuration mode

Usage Guidelines

FCX and ICX devices support configurable shared buffer pools, which help absorb traffic bursts without packet loss. For a given (port, queue) pair, if its buffer usage exceeds the guaranteed limit, it will start using buffers in the shared pool. The shared buffers are apportioned among the 1 Gbps, 10 Gbps, 16 Gbps, and stacking ports.

The **no** form of the command resets the buffer sharing level to the default.

Examples

The following example configures the buffer sharing level to 3.

```
device(config)# qd-share-level 3
```

qos egress-buffer-profile

Configures an egress buffer profile.

Syntax

qos egress-buffer-profile *user-profile-name* **queue-share-level** *level queue-number*

no qos egress-buffer-profile *user-profile-name* **queue-share-level** *level queue-number*

Command Default

The egress buffer profile is:

Queue	Share level
0	level4-1/9
1	level3-1/16
2	level3-1/16
3	level3-1/16
4	level3-1/16
5	level3-1/16
6	level3-1/16
7	level3-1/16

Parameters

user-profile-name

Specifies the name of the egress buffer profile to be configured.

queue-share-level *level*

Specifies the number of buffers that can be used in a sharing pool. Eight levels are supported.

queue-number

Specifies the queue to apply the buffer limit to. There are eight hardware queues per port.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command deletes the egress buffer profile.

You can attach an egress buffer profile to a port.

You must configure the **no qos egress-buffer-profile** command to detach a profile from any ports that are using it before you can configure the **no qos egress-buffer-profile** command to delete it.

The higher the sharing level, the better the port absorb micro-burst. However, higher-sharing levels of 7 and 8 may compromise QoS functions and create uneven distribution of traffic during periods of congestion.

The following eight queue-share levels are supported:

Level	Sharing-pool buffers
level1-1/64	1/64 of buffers in the sharing pool
level2-1/32	1/32 of buffers in the sharing pool
level3-1/16	1/16 of buffers in the sharing pool
level4-1/9	1/9 of buffers in the sharing pool
level5-1/5	1/5 of buffers in the sharing pool
level6-1/3	1/3 of buffers in the sharing pool
level7-1/2	1/2 of buffers in the sharing pool
level8-2/3	2/3 of buffers in the sharing pool

Examples

The following example creates an egress buffer profile named port-40G.

```
Device(config)# qos egress-buffer-profile port-40G queue-share-level
  level1-1/64   1/64 of buffers in the sharing pool
  level2-1/32   1/32 of buffers in the sharing pool
  level3-1/16   1/16 of buffers in the sharing pool
  level4-1/9    1/9 of buffers in the sharing pool
  level5-1/5    1/5 of buffers in the sharing pool
  level6-1/3    1/3 of buffers in the sharing pool
  level7-1/2    1/2 of buffers in the sharing pool
  level8-2/3    2/3 buffers in the sharing pool
```

The following example configures queue 0 on the egress buffer profile named port-40G to use 1/5 of sharing pool.

```
Device(config)# qos egress-buffer-profile port-40G port-40G queue-share-level level5-1/5 0
```

The following example configures queue 1 on the egress buffer profile named port-40G to use 1/64 of the sharing pool.

```
Device(config)# qos egress-buffer-profile port-40G port-40G queue-share-level level1-1/64 1
```

The following example attaches the egress buffer profile named port-40G to ports 1/2/1 to 1/2/6.

```
Device(config)# interface ethernet 1/2/1 to 1/2/6
Device(config-mif-1/2/1-1/2/6)#egress-buffer-profile port-40G
Device(config-mif-1/2/1-1/2/6)#end
```

The following example shows the error if you try to delete a profile that is attached to a port.

```
Device(config)# no qos egress-buffer-profile port-40G
Error - Egress Profile port-40G is active on Port 1/2/1. It must be deactivated from port before
deleting.
```

The following example detaches the egress buffer profile named port-40G from ports 1/2/1 to 1/2/6 and then delete the profile.

```
Device(config)# interface ethernet 1/2/1 to 1/2/6
Device(config-mif-1/2/1-1/2/6)# no egress-buffer-profile port-40G
Device(config-mif-1/2/1-1/2/6)#exit
Device(config)# no qos egress-buffer-profile port-40G
```

History

Release version	Command history
8.0.10	This command was introduced.

qos ingress-buffer-profile

Configures an ingress buffer profile.

Syntax

qos ingress-buffer-profile *user-profile-name* **priority-group** *priority-group-number* **xoff** *shared-level*

no qos ingress-buffer-profile *user-profile-name* **priority-group** *priority-group-number* **xoff** *shared-level*

Command Default

An ingress buffer profile is not configured.

Parameters

user-profile-name
Specifies the name of the ingress buffer profile to be configured.

priority-group *priority-group-number*
Specifies the priority group (PG) number whose XOFF threshold level has to be configured.

xoff *shared-level*
Specifies the per-PG buffer threshold to trigger sending of priority flow control (PFC).

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command deletes the ingress buffer profile.

You can attach an ingress buffer profile to a port.

You must configure the **no qos ingress-buffer-profile** command to detach a profile from any ports that are using it before you can configure the **no qos ingress-buffer-profile** command to delete it.

The higher the sharing level, the better the port absorbs micro-bursts, before reaching the XOFF threshold limit.

If PFC is enabled on PG and per-port with a user-defined ingress buffer profile attached to a port, port max XOFF is 50% of service pool 1. Port max is used as a cap to prevent a port from using too many buffers. Under normal conditions, the PG XOFF limit is reached first.

If a PG is not enabled to send globally, any XOFF value configured has no effect.

The default ingress buffer profiles are as follows:

- For PFC disabled ports, the default PG XOFF limit is level7-1/2
- For PFC enabled ports, the default PG XOFF limit is level2-1/32

The following six PG XOFF limits are supported:

Level	Sharing-pool buffers
level1-1/64	1/64 of buffers in the sharing pool
level2-1/32	1/32 of buffers in the sharing pool
level3-1/16	1/16 of buffers in the sharing pool
level4-1/9	1/9 of buffers in the sharing pool
level5-1/5	1/5 of buffers in the sharing pool
level6-1/3	1/3 of buffers in the sharing pool

Examples

The following example creates an ingress buffer profile for PG 0 with a PG XOFF limit of 1/3 of buffers in the sharing pool.

```
Device(config)#qos ingress-buffer-profile ing1 priority-group 0 xoff level6-1/3
```

History

Release version	Command history
8.0.20	This command was introduced.

qos-internal-trunk-queue

Modifies the dynamic buffer-share level of inter-packet-processor (inter-pp) HiGig links egress queues on ICX 7450 devices.

Syntax

qos-internal-trunk-queue *level queue*

no qos-internal-trunk-queue *level queue*

Command Default

The buffer share level defaults are:

Queue	Share level
0	level4-1/9
1	level3-1/16
2	level3-1/16
3	level3-1/16
4	level3-1/16
5	level3-1/16
6	level3-1/16
7	level3-1/16

Parameters

level

Specifies the number of buffers that can be used in a sharing pool. ICX 7450 devices support eight levels.

queue

Specifies the queue to apply the buffer limit to. Each port has eight hardware queues.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default queue share level on the specified queue.

NOTE
This command is supported only on ICX 7450 devices or across stack units or for ports across master and slave packet-processor (pp) devices in ICX7450-48 units.

The following eight queue-share levels are supported:

Level	Sharing-pool buffers
level1-1/64	1/64 of buffers in the sharing pool

Level	Sharing-pool buffers
level2-1/32	1/32 of buffers in the sharing pool
level3-1/16	1/16 of buffers in the sharing pool
level4-1/9	1/9 of buffers in the sharing pool
level5-1/5	1/5 of buffers in the sharing pool
level6-1/3	1/3 of buffers in the sharing pool
level7-1/2	1/2 of buffers in the sharing pool
level8-2/3	2/3 of buffers in the sharing pool

Examples

The following example configures the buffer share level of inter-packet-processor (inter-pp) HiGig links egress queues.

```
ICX7450-48P Router(config)#qos-internal-trunk-queue
  level1-1/64   1/64 of buffers in the sharing pool
  level2-1/32   1/32 of buffers in the sharing pool
  level3-1/16   1/16 of buffers in the sharing pool
  level4-1/9    1/9 of buffers in the sharing pool
  level5-1/5    1/5 of buffers in the sharing pool
  level6-1/3    1/3 of buffers in the sharing pool
  level7-1/2    1/2 of buffers in the sharing pool
  level8-2/3    2/3 buffers in the sharing pool
```

History

Release version	Command history
08.0.20	This command was introduced.

qos mechanism

Configures the Quality of Service (QoS) queuing method.

Syntax

qos mechanism { **strict** | **weighted** | **mixed-sp-wrr** }

no qos mechanism { **strict** | **weighted** | **mixed-sp-wrr** }

Command Default

By default, the devices use the WRR method of packet prioritization.

Parameters

strict

Changes the method to strict order scheduling.

weighted

Changes the method to weighted scheduling.

mixed-sp-wrr

Changes the method to mixed scheduling using both strict and weighted.

Modes

Global configuration mode

Usage Guidelines

By default, when you select the combined SP and WRR queueing method, the device assigns strict priority to traffic in qosp7 and qosp6, and weighted round robin priority to traffic in qosp0 through qosp5.

The **no** form of the command sets the device to use the WRR method of packet prioritization.

Examples

The following example shows how to change the method to strict priority scheduling.

```
device(config)# qos mechanism strict
```

qos name

Renames the queue.

Syntax

qos name *old-name new-name*

Command Default

The default queue names are qosp7, qosp6, qosp5, qosp4, qosp3, qosp2, qosp1, and qosp0.

Parameters

old-name

Specifies the name of the queue before the change.

new-name

Specifies the new name of the queue. The name can be an alphanumeric string up to 32 characters long.

Modes

Global configuration mode

Examples

The following example shows how to rename the queue " qosp3 " to " 92-octane ".

```
device(config)# qos name qosp3 92-octane
```

qos priority-to-pg

Configures priority-to-priority-group (PG) mapping for priority flow control (PFC).

Syntax

qos priority-to-pg qosp0 *priority-PG-map* **qosp1** *priority-PG-map* **qosp2** *priority-PG-map* **qosp3** *priority-PG-map* **qosp4** *priority-PG-map* **qosp5** *priority-PG-map* **qosp6** *priority-PG-map* **qosp7** *priority-PG-map*

no qos priority-to-pg

Command Default

Priority-to-PG mapping is not configured.

Parameters

qosp0-7

Configures the internal priority based on classification in the range 0 through 7.

priority-PG-map

Specifies the internal priority-to-PG mapping. The range is 0 through 3.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default priority-to-PG map.

You must configure the **priority-flow-control enable** command to enable PFC globally before you configure priority-to-PG mapping.

NOTE

Default mapping, mapping priorities, and mapping restrictions changed in Brocade FastIron Release 8.0.20. The following restrictions apply:

- Priority 7, and only Priority 7, is always mapped to PG4.
- PG4 is always lossy.
- PFC cannot be enabled on PG4.
- Priorities 0 to 5 can be mapped to PG0, PG1, and PG2. They cannot be mapped to PG3 or PG4.

The default value of priority-to-PG maps is:

- QoS internal priority 0 is mapped to PG 0
- QoS internal priority 1 is mapped to PG 0
- QoS internal priority 2 is mapped to PG 1
- QoS internal priority 3 is mapped to PG 1
- QoS internal priority 4 is mapped to PG 1

- QoS internal priority 5 is mapped to PG 2
- QoS internal priority 6 is mapped to PG 2
- QoS internal priority 7 is mapped to PG 4

The default value of priority-to-PG maps in releases prior to Release 8.0.20 is:

- QoS internal priority 0 is mapped to PG 0
- QoS internal priority 1 is mapped to PG 0
- QoS internal priority 2 is mapped to PG 1
- QoS internal priority 3 is mapped to PG 1
- QoS internal priority 4 is mapped to PG 1
- QoS internal priority 5 is mapped to PG 2
- QoS internal priority 6 is mapped to PG 2
- QoS internal priority 7 is mapped to PG 2

In releases prior to Release 8.0.20, you can map QoS internal priority 7 to PG 3. You can also map any other priority to PG 3 if it meets these requirements:

- Lower priorities mapped to lower PGs.
- PGs are configured in ascending order.
- Multiple priorities in a single PG must be consecutive.

Priority-to-PG mapping is not configurable in other modes. Symmetrical and asymmetrical 802.3x flow control modes have their own default priority-to-PG mapping.

You must configure PGs in ascending order, 0 to 3. You can configure a higher-order PG only if all the lower-order PGs have some mapped priorities.

Examples

The following example configures a priority-to-PG map.

```
Device(config)# priority-flow-control enable
Device(config)# qos priority-to-pg qosp0 0 qosp1 1 qosp2 1 qosp3 1 qosp4 2 qosp5 2 qosp6 2 qosp7 4
```

The following example restores the default priority-to-PG map.

```
Device(config)# no qos priority-to-pg qosp0 0 qosp1 1 qosp2 1 qosp3 1 qosp4 2 qosp5 2 qosp6 2 qosp7 4
```

History

Release version	Command history
8.0.10	This command was introduced.
8.0.20	This command was modified to change priority 7-to-PG4 mapping and mapping restrictions for priorities 0 through 5.

qos profile

Changes the minimum bandwidth percentages of the Weighted Round Robin (WRR) queues.

Syntax

qos profile *name7* { **sp** | *percentage* } *name6* { **sp** | *percentage* } *name5* { **sp** | *percentage* } *name4* { **sp** | *percentage* } *name3* { **sp** | *percentage* } *name2* { **sp** | *percentage* } *name1* { **sp** | *percentage* } *name0* { **sp** | *percentage* }

no qos profile *name7* { **sp** | *percentage* } *name6* { **sp** | *percentage* } *name5* { **sp** | *percentage* } *name4* { **sp** | *percentage* } *name3* { **sp** | *percentage* } *name2* { **sp** | *percentage* } *name1* { **sp** | *percentage* } *name0* { **sp** | *percentage* }

Command Default

The eight QoS queues on FastIron devices receive the minimum guaranteed percentages of a port's total bandwidth, as shown in the following table . Note that the defaults differ when jumbo frames are enabled.

Parameters

name

Specifies the name of a queue. You can specify the queues in any order on the command line, but you must specify each queue.

sp

Changes the method to strict priority scheduling.

percentage

Specifies a number for the percentage of the device outbound bandwidth that is allocated to the queue. QoS queues require a minimum bandwidth percentage of 3 percent for each priority. When jumbo frames are enabled, the minimum bandwidth requirement is 8 percent. If these minimum values are not met, QoS may not be accurate.

Modes

Global configuration mode

Usage Guidelines

When the queuing method is WRR, the software internally translates the percentages into weights. The weight associated with each queue controls how many packets are processed for the queue at a given stage of a cycle through the weighted round robin algorithm.

TABLE 8 Default minimum bandwidth percentages on the devices

Queue	Default minimum percentage of bandwidth	
	Without jumbo frames	With jumbo frames
qosp7	75%	44%
qosp6	7%	8%
qosp5	3%	8%
qosp4	3%	8%
qosp3	3%	8%
qosp2	3%	8%

TABLE 8 Default minimum bandwidth percentages on the devices (continued)

Queue	Default minimum percentage of bandwidth	
qosp1	3%	8%
qosp0	3%	8%

The **no** form of the command returns to the default bandwidth percentages.

Examples

The following example shows how to change the bandwidth percentages for the queues.

```
device(config)#qos profile qosp7 25 qosp6 15 qosp5 12 qosp4 12 qosp3 10 qosp2
10 qosp1 10 qosp0 6

Profile qosp7 : Priority7 bandwidth requested 25% calculated 25%
Profile qosp6 : Priority6 bandwidth requested 15% calculated 15%
Profile qosp5 : Priority5 bandwidth requested 12% calculated 12%
Profile qosp4 : Priority4 bandwidth requested 12% calculated 12%
Profile qosp3 : Priority3 bandwidth requested 10% calculated 10%
Profile qosp2 : Priority2 bandwidth requested 10% calculated 10%
Profile qosp1 : Priority1 bandwidth requested 10% calculated 10%
Profile qosp0 : Priority0 bandwidth requested 6% calculated 6%
```

qos scheduler-profile

Configures a user-defined Quality of Service (QoS) scheduler profile.

Syntax

qos scheduler-profile *user-profile-name* { **mechanism** *scheduling-mechanism* | **profile** [**qosp0** *wt0* | **qosp1** *wt1* | **qosp2** *wt2* | **qosp3** *wt3* | **qosp4** *wt4* | **qosp5** *wt5* | **qosp6** *wt6* | **qosp7** *wt7*] }

no qos scheduler-profile *user-profile-name*

Command Default

A user-defined QoS scheduler profile is not configured.

Parameters

user-profile-name

Specifies the name of the scheduler profile to be configured.

mechanism *scheduling-mechanism*

Configures the queue assignment with the specified scheduling mechanism. The following scheduling mechanisms are supported:

mixed-sp-wrr

Specifies mixed strict-priority (SP) and weighted scheduling.

strict

Specifies SP scheduling.

weighted

Specifies weighted scheduling.

profile qosp0-7

Configures the profile based on classification in the range 0 through 7.

wt0-7

Specifies the bandwidth percentage for the corresponding QoS profile. The range is from 0 through 7.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command removes the scheduler profile configuration.

You can use the **scheduler-profile** command to attach a user scheduler profile to a port. If you want to remove a scheduler-profile you must ensure that it is not attached to any port.

On ICX 7750 and ICX 7450 devices, changing the global scheduler and port scheduler on running traffic may cause traffic loss.

The default QoS-profile weights for each queue using a weighted QoS mechanism are as follows:

Profile	Priority	Weighted bandwidth
Profile qosp7	Priority7(Highest)	Bandwidth requested 44% calculated 44%
Profile qosp6	Priority6	Bandwidth requested 8% calculated 8%
Profile qosp5	Priority5	Bandwidth requested 8% calculated 8%
Profile qosp4	Priority4	Bandwidth requested 8% calculated 8%
Profile qosp3	Priority3	Bandwidth requested 8% calculated 8%
Profile qos2	Priority2	Bandwidth requested 8% calculated 8%
Profile qosp1	Priority1	Bandwidth requested 8% calculated 8%
Profile qosp0	Priority0 (Lowest)	Bandwidth requested 8% calculated 8%

Per-queue details	Bandwidth percentage
Class 0	3
Class 1	3
Class 2	3
Class 3	3
Class 4	3
Class 5	3
Class 6	7
Class 7	75

The default QoS-profile weights for each queue using a mixed QoS mechanism are as follows:

Per-queue details	Bandwidth percentage
Class 0	15
Class 1	15
Class 2	15
Class 3	15
Class 4	15
Class 5	25
Class 6	sp
Class 7	sp

The total weight (wt0-wt7) in both weighted and mixed mechanism must be 100 percent.

The minimum value for any weight is 1.

A maximum of eight scheduler profiles are supported.

Examples

The following example configures a QoS scheduler profile named user1, with weighted scheduling, and specify the bandwidth percentage for each QoS class:.

```
Device(config)# qos scheduler-profile user1 mechanism weighted
Device(config)# qos scheduler-profile user1 profile qosp0 1 qosp1 1 qosp2 10 qosp3 10 qosp4 10 qosp5 10
qosp6 20 qosp7 38
```

The following example configures a QoS scheduler profile named user2, with SP scheduling.

```
Device(config)# qos scheduler-profile user2 mechanism strict
```

The following example configures a QoS scheduler profile named user3, with mixed SP and weighted scheduling.

```
Device(config)# qos scheduler-profile user3 mechanism mixed-sp-wrr
```

The following example removes a QoS scheduler profile named user3.

```
Device(config)# no qos scheduler-profile user3
```

History

Release version	Command history
08.0.10	This command was introduced.

qos tagged-priority

Changes the VLAN priority 802.1p to hardware forwarding queue mappings.

Syntax

qos tagged-priority *num queue*

no qos tagged-priority *num queue*

Parameters

num

Specifies the VLAN priority. The value can range from 0 to 7.

queue

Specifies the hardware forwarding queue to which you are reassigning the priority. The default queue names are as follows: qosp7, qosp6, qosp5, qosp4, qosp3, qosp2, qosp1, qosp0.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command sets the VLAN priority to 802.1p.

Examples

The following example shows how to map the VLAN priority 2 to the hardware forwarding queue qosp0.

```
device(config)# qos tagged-priority 2 qosp0
```

qos-tos map dscp-priority

Changes the DSCP to internal forwarding priority mappings.

Syntax

qos-tos map dscp-priority *dscp-value1 dscp-value2 dscp-value3 dscp-value4 dscp-value5 dscp-value6 dscp-value7 dscp-value8* **to** *priority*

no qos-tos map dscp-priority *dscp-value1 dscp-value2 dscp-value3 dscp-value4 dscp-value5 dscp-value6 dscp-value7 dscp-value8* **to** *priority*

Command Default

Refer the Usage Guidelines.

Parameters

dscp-value

Specifies the DSCP value ranges you are remapping. You can specify up to eight DSCP values in the same command, to map to the same forwarding priority.

priority

Specifies the internal forwarding priority.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command returns to the default value.

TABLE 9 Default DSCP to internal forwarding priority mappings

Internal forwarding priority	DSCP value
0 (lowest priority queue)	0 - 7
1	8 - 15
2	16 - 23
3	24 - 31
4	32 - 39
5	40 - 47
6	48 - 55
7 (highest priority queue)	56 - 63

DSCP values range from 0 through 63, whereas the internal forwarding priority values range from 0 through 7. Any DSCP value within a given range is mapped to the same internal forwarding priority value. For example, any DSCP value from 8 through 15 maps to priority 1.

Examples

The following example shows how to change the DSCP to internal forwarding priority mappings.

```
device(config)# qos-tos map dscp-priority 0 2 3 4 to 1
```

radius-client coa host

Configures the key to be used between the Change of Authorization (CoA) client and FastIron device.

Syntax

radius-client coa host { *addr* | *name* } [**key** *key-string*]

no radius-client coa host { *addr* | *name* } [**key** *key-string*]

Command Default

No key is configured between the CoA client and device.

Parameters

addr

Address of the CoA host.

name

Name of the CoA host.

key *key-string*

The key required to be used between the CoA client and FastIron device.

Modes

Global configuration mode

Usage Guidelines

no

RADIUS Change of Authorization (CoA) messages from clients configured through this command will be processed. CoA messages from unconfigured clients will be discarded.

Examples

The following example displays the configuration between CoA host and the device.

```
device(config)# radius-client coa host 10.21.240.46 key 0 Foundry1#
```

History

Release version	Command history
08.0.20	This command was introduced.

radius-client coa port

Changes the default CoA (Change of Authorization) port number.

Syntax

radius-client coa port *udp-port-number*

no radius-client coa port *udp-port-number*

Command Default

The CoA port number is 3799.

Parameters

udp-port-number
The number of the UDP port.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command restores the default port number (3799).

Examples

The following example changes the CoA port number to 3000.

```
device(config)# radius-client coa port 3000
```

History

Release version	Command history
08.0.20	This command was introduced.

rp-embedded

Configures embedded-rendezvous point (RP) support on PIM devices.

Syntax

rp-embedded

no rp-embedded

Command Default

Embedded RP support is enabled.

Modes

PIM router configuration mode

PIM router VRF configuration mode

Usage Guidelines

The **no** form of this command disables embedded RP support.

Examples

This example disables embedded RP support.

```
Device(config)# ipv6 router pim
Device(config-ipv6-pim-router)#no rp-embedded
```

This example disables embedded RP support on a VRF named blue.

```
Device(config)#ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)#no rp-embedded
```

radius-server enable

Configures the device to allow RADIUS server management access only to clients connected to ports within the port-based VLAN.

Syntax

radius-server enable vlan *vlan-number*

no radius-server enable vlan *vlan-number*

Command Default

By default, access is allowed on all ports.

Parameters

vlan *vlan-number*

Configures access only to clients connected to ports within the VLAN.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the restriction.

You can restrict management access to a Brocade device to ports within a specific port-based VLAN. VLAN-based access control works in conjunction with other access control methods. Clients connected to ports that are not in the VLAN are denied management access.

Examples

The following example shows how to allow RADIUS server access only to clients in a specific VLAN.

```
device(config)# radius-server enable vlan 10
```

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**] [**port-only**]]]]]

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**] [**port-only**]]]]]

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 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. TLS-encrypted sessions support both IPv4 and IPv6.

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.

port-only
The **port-only** parameter is optional and specifies that the server will be used only to authenticate users on ports to which it is mapped.

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 the RADIUS key for each server.

TLS-encrypted TCP sessions are not supported by management VRF.

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 configures non-default UDP ports for authorization and accounting.

```
device(config)#radius-server host 1.2.3.4 auth-port 100 acct-port 200
device(config)#sh aaa
***** TACACS server not configured
Radius default key: ...
Radius retries: 3
Radius timeout: 3 seconds
Radius Server:          IP=172.26.67.12 SSL Port=2083 Usage=any
                   Key=...
                   opens=0 closes=0 timeouts=0 errors=0
                   packets in=0 packets out=0
                   IPv4 Radius Source address: IP=0.0.0.0              IPv6 Radius Source
Address:           IP=::
Radius Server:          IP=1.2.3.4 Auth Port=100 Acct Port=200 Usage=any
                   Key=...
                   opens=0 closes=0 timeouts=0 errors=0
                   packets in=0 packets out=0
                   IPv4 Radius Source address: IP=0.0.0.0              IPv6 Radius Source
Address:           IP=::
```

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 configure RADIUS server for TLS support.

```
device(config)# radius-server host 172.26.67.12 ssl-auth-port 2083 default key whatever
device(config)#sh aaa
***** TACACS server not configured
Radius default key: ...
Radius retries: 3
Radius timeout: 3 seconds
Radius Server:          IP=172.26.67.12 SSL Port=2083 Usage=any
                   Key=...
                   opens=0 closes=0 timeouts=0 errors=0
                   packets in=0 packets out=0
                   IPv4 Radius Source address: IP=0.0.0.0              IPv6 Radius Source
Address:           IP=::
```

radius-server key

Configures the value that the device sends to the RADIUS server when trying to authenticate user access.

Syntax

radius-server key *key-string*

no radius-server key *key-string*

Command Default

The RADIUS server key is not configured.

Parameters

key-string

Specifies the key as an ASCII string. The value for the key parameter on the Brocade device should match the one configured on the RADIUS server. The key can be from 1 through 64 characters in length and cannot include any space characters.

Modes

Global configuration mode

Usage Guidelines

The **radius-server key** command is used to encrypt RADIUS packets before they are sent over the network.

The **no** form of the command removes the RADIUS server key configuration.

Examples

The following example shows how to configure a RADIUS server key.

```
device(config)# radius-server key abc
```

radius-server retransmit

Configures the maximum number of retransmission attempts for a request when a RADIUS authentication request times out.

Syntax

radius-server retransmit *number*

no radius-server retransmit *number*

Command Default

The default retransmit number is three retries.

Parameters

number

The maximum number of retries the Brocade software retransmits the request. The valid values are from 1 through 5. The default is 3.

Modes

Global configuration mode

Usage Guidelines

When an authentication request times out, the Brocade software retransmits the request up to the maximum number of retransmission tries configured.

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

Examples

The following example shows how to set the retransmission number to 4.

```
device(config)# radius-server retransmission 4
```

radius-server timeout

Configures the number of seconds the Brocade device waits for a response from a RADIUS server before either retrying the authentication request, or determining that the RADIUS servers are unavailable and moving on to the next authentication method in the authentication method list.

Syntax

radius-server timeout *time*

no radius-server timeout *time*

Command Default

The default timeout value is 3 seconds.

Parameters

time

The timeout value in seconds. Valid values are from 1 through 15 seconds. The default is 3 seconds.

Modes

Global configuration mode

Usage Guidelines

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

Examples

The following example shows how to set the RADIUS server timeout value to 10 seconds.

```
device(config)# radius-server timeout 10
```

raguard

Configures the current interface as a trusted, untrusted, or host Router Advertisement (RA) guard port.

Syntax

raguard { **trust** | **untrust** | **host** }

no raguard { **trust** | **untrust** | **host** }

Parameters

trust
Configures an interface as a trusted RA guard port.

untrust
Configures an interface as an untrusted RA guard port.

host
Configures an interface as a host RA guard port.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command removes the current trusted or untrusted configuration.

A trusted RA guard port forwards all the receive RA packets without inspecting. An untrusted port inspects the received RAs against the RA guard policy's whitelist, prefix list and preference maximum settings before forwarding the RA packets. If an RA guard policy is not configured on an untrusted or host port, all the RA packets are forwarded.

Examples

The following example configures an interface as a trusted RA guard port:

```
Brocade(config)# interface ethernet1/1/1
Brocade(config-int-e1000-1/1/1)# raguard trust
```

The following example configures an interface as an untrusted RA guard port:

```
Brocade(config)# interface ethernet1/2/1
Brocade(config-int-e1000-1/2/1)# raguard untrust
```

The following example configures an interface as a host RA guard port:

```
Brocade(config)# interface ethernet3/2/1
Brocade(config-int-e1000-3/2/1)# raguard host
```

rate-limit input

Configures a port-based rate-limiting policy.

Syntax

rate-limit input fixed *average-rate* [**burst** *burst-size*]

no rate-limit input fixed *average-rate* [**burst** *burst-size*]

rate-limit input fixed ethe *stack/slot /port average-rate*

no rate-limit input fixed ethe *stack/slot /port average-rate*

Parameters

fixed

Configures fixed rate-limiting policy.

average-rate

Specifies the maximum number of kilobits per second (kbps).

burst *burst-size*

Specifies the burst size in kilobits.

Modes

Interface configuration mode

LAG configuration mode

Usage Guidelines

The **no** form of the command removes rate limiting.

Examples

The following example configures rate limiting on a port.

```
device(config)# interface ethernet 1/1/2
device(config-if-e1000-1/1/2)# rate-limit input fixed 500
```

rate-limit output

Configures the maximum rate at which outbound traffic is sent out on a port priority queue or on a LAG port.

Syntax

rate-limit output shaping *value* [**priority** *priority-queue*]

no rate-limit output shaping *value* [**priority** *priority-queue*]

rate-limit output shaping ethe *stackid/slot/port value* [**priority** *priority-queue*]

no rate-limit output shaping ethe *stackid/slot/port value* [**priority** *priority-queue*]

Parameters

shaping *value*

Specifies the rate shaping limit.

ethernet *stackid/slot/port*

Specifies the Ethernet port.

priority *priority-queue*

Specifies Rate Shaping for specific priority. The value can range from 0 to 7.

Modes

Interface configuration mode

LAG configuration mode

Usage Guidelines

The **no** form of the command removes the output rate shaping.

Examples

The following example shows how to configure the maximum rate at which outbound traffic is sent out on a port priority queue

```
device(config)# interface ethernet 1/2/1
device(config-if-e1000-1/2/1)# rate-limit output shaping 500 priority 7
```

The following example shows how to configure the maximum rate at which outbound traffic is sent out on a LAG port.

```
device(config)# lag lag1 static
device(config-lag-lag1)# rate-limit output shaping ethernet 1/1/15 651
```

rate-limit-log

Configures the global level BUM suppression logging interval.

Syntax

rate-limit-log [*minutes*]

[no] rate-limit-log [*minutes*]

Command Default

The default logging interval 5 minutes.

Parameters

minutes

Specifies the interval, in whole mimutes, between Syslog notifications. The value can be any integer from 1 to 10.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to return to the default value (5 minutes).

Examples

The following example shows how to set the BUM suppression notification Syslog logging interval to 3 minutes.

```
device(config)# rate-limit-log 3
```

History

Release version	Command history
8.0.30h	This command was introduced.

rbridge-id

Configures the cluster or cluster client RBridge ID.

Syntax

rbridge-id *rbridge-id*

no rbridge-id *rbridge-id*

Command Default

An RBridge ID is not configured.

Parameters

rbridge-id

Specifies the RBridge ID of the cluster or client. The valid values are from 1 through 4095.

Modes

Cluster configuration mode

Cluster client configuration mode

Usage Guidelines

Use this command to configure the cluster or cluster client RBridge ID. The RBridge ID is a value assigned to MCT cluster devices and clients that uniquely identifies them and helps associate the source MAC address with an MCT device.

The cluster RBridge ID and cluster client RBridge ID should be unique. The two IDs should not conflict with each other or with the cluster ID or client ID.

The **no** form of the command removes the RBridge ID.

Examples

The following example configures the cluster RBridge ID.

```
device(config)# cluster SX 4000
device(config-cluster-SX)# rbridge-id 3
```

rconsole

Use the **rconsole command** to establish a remote console session with a stack member.

Syntax

rconsole *stack-unit*

Command Default

N/A

Parameters

stack-unit

Stack-unit ID of the remote device

Modes

Privileged EXEC mode.

Usage Guidelines

You can terminate a session in any of these ways:

- by entering the **exit** command from the User EXEC level
- by entering the **logout** command at any level.

Examples

To establish an rconsole session, enter the **rconsole** command as shown:

```
device# rconsole 1
```

In the following example, a remote console session is established with stack unit 2.

```
device# rconsole 2
Connecting to unit 2... (Press Ctrl-O X to exit)
rconsole-2@device# show stack
ID   Type    Role      Mac Address      Prio State    Comment
2  S FCX624P standby   0000.00e2.ba40           0    local    Ready
rconsole-2@device# exit
rconsole-2@device> exit
Disconnected.  Returning to local session...
```

History

Release version	Command history
FastIron release 08.0.00a	This command was introduced.

rd

Distinguishes a route for VRF.

Syntax

rd {*ASN:nn* | *IP-address:nn* }

Parameters

ASN:nn

Configures the RD as AS number followed by a colon (:) and a unique arbitrary number.

IP-address:nn

Configures the RD as IP address followed by a colon (:) and a unique arbitrary number.

Modes

VRF configuration mode

Usage Guidelines

Each VRF instance is identified by a unique Route Distinguisher (RD). The RD is prepended to the address being advertised. Because the RD provides overlapping client address space with a uniqueidentifier, the same IP address can be used in different VRFs without conflict. The RD can be an AS number, followed by a colon (:) and a unique arbitrary number as in "10:11". Alternatively, it canbe a local IP address followed by a colon (:) and a unique arbitrary number, as in "1.1.1.1:100".

Once the Route Distinguisher is configured for a VRF it cannot be changed or deleted. To remove the Route Distinguisher, you must delete the VRF.

Examples

The following example shows how to configure a Route Distinguisher.

```
device(config)# vrf red
sevice(config-vrf-red)# rd 101:101
```

re-authentication (802.1x authentication)

Configures the device to periodically re-authenticate the clients connected to 802.1X-enabled interfaces at regular interval.

Syntax

re-authentication

no re-authentication

Command Default

The device re-authenticates the clients connected to 802.1X-enabled interfaces every 3,600 seconds.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command disables the periodic re-authentication of the clients connected to 802.1X-enabled interfaces.

When the periodic reauthentication is enabled, the device reauthenticates the clients every 3,600 seconds by default. If the reauthentication interval is configured using the **re-auth period** command, reauthentication happens at that interval.

Examples

The following example configures the device to re-authenticate the clients connected to 802.1X-enabled interfaces every 3,600 seconds.

```
device(config)# dot1x-enable
device(config-dot1x)# re-authentication
```

History

Release version	Command history
08.0.20	This command was replaced on Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750 by the **re-authentication (Flexible authentication)** command.

re-authentication (Flexible authentication)

Periodically reauthenticates clients connected to 802.1X and MAC-authentication enabled interfaces.

Syntax

re-authentication

no re-authentication

Command Default

Reauthentication is not enabled.

Modes

Authentication configuration mode

Usage Guidelines

The **no** form of this command disables re-authentication.

When periodic reauthentication is enabled, the device reauthenticates clients every 3,600 seconds by default. The reauthentication interval configured by using the **reauth-period** command takes precedence.

Examples

The following example configures periodic re-authentication using the default interval of 3,600 seconds.

```
device(config)# authentication
device(config-authen)# re-authentication
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.30mb	Reauthentication support was added to MAC-authentication enabled ports.

reauth-period

Configures the interval at which clients connected to 802.1X and MAC-authentication enabled ports are reauthenticated.

Syntax

reauth-period *seconds*

no reauth-period*seconds*

Command Default

The reauthentication period is 3600 seconds.

Parameters

seconds

Sets the reauthentication period. The range is 1 through 4294967295 seconds.

Modes

Authentication configuration mode

Usage Guidelines

While the **re-authentication** command configures periodic re-authentication using the default interval of 3600 seconds, the **reauth-period** command allows you to specify a value in seconds.

The reauthentication interval configured by using the **reauth-period** command can be overwritten for each client by the RADIUS server through the Session-Timeout and Termination-Action attributes. For example, a session is reauthenticated when it receives a RADIUS session-timeout message because the RADIUS session-timeout is prioritized over the reauthentication interval that is configured by using the **reauth-period** command.

The **no** form of this command reverts the re-authentication period to the default interval of 3600 seconds.

Examples

The following example configures periodic reauthentication with an interval of 2,000 seconds.

```
device(config)# authentication
device(config-authen)# re-authentication
device(config-authen)# reauth-period 2000
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.30mb	Reauthentication support was added to MAC-authentication enabled ports.

reauth-time

Configures the number of seconds an authenticated user remains authenticated.

Syntax

reauth-time *seconds*

no reauth-time *seconds*

Command Default

The default is 28,800 seconds.

Parameters

seconds

The number of seconds an authenticated user remains authenticated. The valid values are from 0 through 128,000 seconds. The default is 28,800.

Modes

Web Authentication configuration mode

Usage Guidelines

After a successful authentication, a user remains authenticated for a duration of time. At the end of this duration, the host is automatically logged off. The user must be reauthenticated again.

Setting a value of 0 means the user is always authenticated and will never have to reauthenticate, except if an inactive period less than the reauthentication period is configured on the Web Authentication VLAN. If this is the case, the user becomes deauthenticated if there is no activity and the timer for the inactive period expires.

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

Examples

The following example configures the reauthentication time as 300 seconds.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# reauth-time 300
```

redistribute ospf

Configures the device to redistribute OSPF routes into BGP.

Syntax

redistribute ospf [**match** [**external1** | **external2** | **internal**]] [**metric** *num*] [**route-map** *string*]

no redistribute ospf [**match** [**external1** | **external2** | **internal**]] [**metric** *num*] [**route-map** *string*]

Command Default

Internal OSPF routes are distributed. No value is assigned for **metric**.

Parameters

match
: Selects the type of route to be redistributed.

external1
: Redistributes OSPF external type 1 routes.

external2
: Redistributes OSPF external type 2 routes.

internal
: Redistributes OSPF internal routes.

num
: A value that assigns the metric.The range is from 0 through 4294967297.

string
: Specifies a route map to be consulted before an OSPF route is added to the BGP routing table.

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

Usage Guidelines

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

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.

Use the **redistribute ospf** command to redistribute all OSPF routes (OSPF external type 1, external type 2, or internal routes).

Examples

This example redistributes IPv4 OSPF external type 1 routes with a metric of 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# redistribute ospf match external1 metric 200
```

This example redistributes OSPF IPv6 external type 2 routes in a nondefault VRF instance.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# redistribute ospf match external2
```

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

redistribute (BGP)

Configures the device to redistribute RIP routes, directly connected routes, or static routes into BGP4 and BGP4+.

Syntax

redistribute { **connected** | **rip** | **static** } [**metric** *num*] [**route-map** *string*]

no redistribute { **connected** | **rip** | **static** } [**metric** *num*] [**route-map** *string*]

Command Default

The device does not redistribute routing information between BGP4 or BGP4+ and the IP interior gateway protocol OSPF.

Parameters

connected
Redistributes connected routes.

rip
Redistributes Routing Information Protocol (RIP) routes.

static
Redistributes static routes.

metric
Metric for redistributed routes.

num
Specifies a metric number. The range is from 0 through 4294967297. No value is assigned by default.

route-map
Specifies that a route map be consulted before a route is added to the routing table.

string
Specifies a route map to be consulted before a route is added to the routing table.

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

Usage Guidelines

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

Use this command to configure the device to redistribute RIP, directly connected routes, or static routes into BGP4 or BGP4+. The routes can be filtered by means of an associated route map before they are distributed.

NOTE
The **default-metric** command does not apply to the redistribution of directly connected routes into BGP4 or BGP4+. Use a route map to change the default metric for directly connected routes.

Examples

This example redistributes static routes into BGP4 and specifies a metric of 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# redistribute static metric 200
```

This example redistributes static routes into BGP4+ and specifies that route-map "rm5" be consulted.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# redistribute route-map rm5
```

This example redistributes directly connected routes into BGP4 in VRF instance "red".

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

History

Release version	Command history
8.0.30	Support was added for the BGP address-family IPv6 unicast VRF configuration mode.

register-probe-time

Configures the time the PIM router waits for a register-stop from a rendezvous point (RP) before it generates another NULL register to the PIM RP

Syntax

register-probe-time *seconds*

no register-probe-time *seconds*

Command Default

The wait time is10 seconds.

Parameters

seconds

Specifies the time, in seconds, between queries. The range is 10 through 50 seconds. The default is 10 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the wait time to 10 seconds.

The register-probe time configuration applies only to the first-hop PIM router.

NOTE
When a PIM first-hop router has successfully registered with a PIM RP, the PIM first-hop router will not default back to the data registration. All subsequent registers will be in the form of the NULL registration.

Examples

This example configures the register-probe time to 20 seconds.

```
Device(config)#router pim
Device(config-pim-router)#register-probe-time 20
```

register-suppress-time

Configures the interval at which the PIM router triggers the NULL register message.

Syntax

register-suppress-time *seconds*

no register-suppress-time *seconds*

Command Default

The interval at which PIM router triggers the NULL register message is 60 seconds.

Parameters

seconds

Specifies the interval, in seconds, between queries. The range is 60 through 120 seconds. The default is 60 seconds.

Modes

PIM router configuration mode

Usage Guidelines

The **no** form of this command restores the register-suppress interval to 60 seconds.

The register-suppress interval configuration applies only to the first-hop PIM router.

Examples

The following example configures the interval at which PIM router triggers the NULL register message to 90 seconds.

```
Device(config)#router pim
Device(config-pim-router)#register-suppress-time 90
```

relative-utilization

Configures uplink utilization lists that display the percentage of a given uplink port bandwidth that is used by a specific list of downlink ports.

Syntax

relative-utilization *number* **uplink ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...] **downlink ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no relative-utilization *number* **uplink ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...] **downlink ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

Relative utilization is not configured.

Parameters

number
Specifies the list number. The value can range from 1 to 4. You can specify upto 4 lists.

uplink ethernet *stackid/slot/port*
Specifies the uplink ethernet port.

to *stackid/slot/port*
Specifies a range of ethernet ports.

downlink ethernet *stackid/slot/port*
Specifies the downlink ethernet port.

Modes

Global configuration mode

Usage Guidelines

Each uplink utilization list consists of the following:

- Utilization list number (1, 2, 3, or 4).
- One or more uplink ports.
- One or more downlink ports.

Each list displays the uplink port and the percentage of that port bandwidth that was utilized by the downlink ports over the most recent 30-second interval.

You can configure up to four bandwidth utilization lists.

You can specify a list or range of ports as uplink or downlink ports.

The **no** form of the command removes the uplink utilization list.

Examples

The following example shows how to configure the uplink utilization list.

```
device(config)# relative-utilization 1 uplink ethernet 1/1/1 downlink ethernet 1/2/2 to 1/3/2
```

remark

Adds a comment to describe entries in an IPv4 or IPv6 ACL.

Syntax

remark *comment-text*

no remark *comment-text*

Command Default

No comments are added to describe entries in an IPv4 or IPv6 ACL.

Parameters

comment-text

Specifies the comment for the ACL entry, up to 256 alphanumeric characters.

Modes

IPv4 access list configuration mode

IPv6 access list configuration mode

Usage Guidelines

You can add a comment by entering the **remark** command immediately preceding an ACL entry. The comment appears in the output of show commands that display ACL information.

The **no** form of the command deletes the comment text added for an ACL entry.

Examples

The following example configures remarks for an IPv4 ACL.

```
device(config)# ip access-list extended TCP/UDP
device(config-ext-nacl)# remark The following line permits TCP packets
device(config-ext-nacl)# permit tcp 192.168.4.40/24 2.2.2.2/24
device(config-ext-nacl)# remark The following permits UDP packets
device(config-ext-nacl)# permit udp 192.168.2.52/24 2.2.2.2/24
device(config-ext-nacl)# deny ip any any
```

The following example configures remarks for an IPv6 ACL.

```
device(config)# ipv6 access-list rtr
device(config-ipv6-access-list rtr)# remark This entry permits ipv6 packets from 2001:DB8::2 to any
destination
device(config-ipv6-access-list rtr)# permit ipv6 host 2001:DB8::2 any
device(config-ipv6-access-list rtr)# remark This entry denies udp packets from any source to any
destination
device(config-ipv6-access-list rtr)# deny udp any any
device(config-ipv6-access-list rtr)# remark This entry denies IPv6 packets from any source to any
destination
device(config-ipv6-access-list rtr)# deny ipv6 any
```

The following example shows the comment text for the ACL named "rtr" in a show running-config display.

```
device# show running-config
ipv6 access-list rtr
remark This entry permits ipv6 packets from 2001:DB8::2 to any destination permit ipv6 host 2001:DB8::2
any
remark This entry denies udp packets from any source to any destination deny udp any any
remark This entry denies IPv6 packets from any source to any destination deny ipv6 any any
```

The following example shows how to delete a comment from an IPv6 ACL entry.

```
device(config)# ipv6 access-list rtr
device(config-ipv6-access-list rtr)# no remark This entry permits ipv6 packets from 2001:DB8::2 to any
destination
```

remote-loopback

Starts or stops the remote loopback procedure on a remote device.

Syntax

remote-loopback ethernet *stackid/slot/port* { **start** | **stop** }

Command Default

Remote loopback is not initiated on a remote device.

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet interface on which loopback is to be enabled.

start

Starts the remote loopback procedure on a remote device.

stop

Stops the remote loopback procedure on a remote device.

Modes

EFM-OAM protocol configuration mode

Usage Guidelines

The **remote-loopback ethernet** *stackid/slot/port* { **start** | **stop** } command is valid only on the Data Terminal Equipment (DTE) operating in the active mode.

When the remote loopback mode is enabled, all the non-OAMPDUs are looped back at the remote end.

A port ceases to be in the remote loopback mode if any event triggers a change in the port status (up or down).

If EEE is enabled globally, port ceases to be in the remote loopback mode.

Ethernet loopback and EFM-OAM remote loopback cannot be configured on the same interface.

NOTE
Brocade recommends to ensure that any higher layer protocol running over the local and remote loopback ports does not block the interfaces in the VLAN on which loopback traffic testing is being performed.

Examples

The following example initiates the remote loopback procedure on a remote DTE.

```
device(config)# link-oam
device(config-link-oam)# remote-loopback ethernet 3/1/1 start
```

The following example stops the remote loopback procedure on a remote DTE.

```
device(config)# link-oam
device(config-link-oam)# remote-loopback ethernet 3/1/1 stop
```

History

Release version	Command history
08.0.30	This command was introduced.

reserved-vlan-map

Assigns a different VLAN ID to the reserved VLAN.

Syntax

reserved-vlan-map vlan *vlan-id* **new-vlan** *vlan-id*

no reserved-vlan-map vlan *vlan-id* **new-vlan** *vlan-id*

Command Default

The reserved VLAN ID are 4091 and 4092.

Parameters

vlan *vlan-id*

Specifies the default reserved VLAN ID.

new-vlan *vlan-id*

Specifies the new VLAN ID that you want to assign to the reserved VLAN.

Modes

Global configuration mode

Usage Guidelines

For *vlan-id*, enter a valid VLAN ID that is not already in use. Valid VLAN IDs are numbers from 1 through 4090, 4093, and 4095. VLAN ID 4094 is reserved for use by Single STP.

NOTE

You must save the configuration (**write memory**) and reload the software to place the change into effect.

The **no** form of the command resets the values back to the default reserved VLAN IDs.

Examples

The following example shows how to assign a new VLAN ID to the reserved VLAN IDs.

```
device(config)# reserved-vlan-map vlan 4091 new-vlan 10
Reload required. Please write memory and then reload or power cycle.
device(config)# write memory
device(config)# exit
device# reload
```

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
```

restart-vsrp-port

Configures a single port on a VSRP-configured device to shut down when a failover occurs and restart after a period of time.

Syntax

restart-vsrp-port *seconds*

no restart-vsrp-port *seconds*

Command Default

The default is 1 second.

Parameters

seconds

Configures the VSRP master to shut down its port for the specified number of seconds 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.

Examples

The following example configures the VSRP port to restart in 5 seconds.

```
device(config)# interface ethernet 1/1/1
device(config-if-e-10000)# restart-vsrp-port 5
```

restricted-vlan

Configures a specific VLAN as the restricted VLAN for all ports on the device to place the client port when the authentication fails.

Syntax

restricted-vlan *vlan-id*

no restricted-vlan *vlan-id*

Command Default

The restricted VLAN is not configured.

Parameters

vlan-id

Specifies the identification number of the restricted VLAN.

Modes

Authentication configuration mode

Usage Guidelines

When an authentication fails, the port can be moved into a configured restricted VLAN instead of blocking the client completely. The port is moved to the configured restricted VLAN only if the authentication failure action is set to place the port in a restricted VLAN using the **auth-fail-action** command at the global level or using the **authentication fail-action** command at the interface level. Else, when the authentication fails, the client's MAC address is blocked in the hardware (default action).

The **no** form of the command disables the restricted VLAN.

Examples

The following example creates a restricted VLAN with VLAN 4.

```
device(config)# authentication
device(config-authen)# restricted-vlan 4
```

History

Release version	Command history
08.0.20	This command was introduced.

reverse-path-check

Enables strict mode unicast Reverse Path Forwarding for all layer 3 routes.

Syntax

reverse-path-check

no reverse-path-check

Command Default

Reverse path check is not enabled on the device.

Modes

Global configuration mode

Usage Guidelines

On ICX 6610 devices, this command configures strict mode so that IPv4 prefixes learned over the VE interfaces that do not have tunnel termination specified as next hop are enabled for uRPF check. On ICX 7750 devices, this command enables the uRPF command line interface and hardware settings.

The **no** form of the command disables the reverse path check functionality.

You must reload the device for the reverse path check setting changes to take effect. Enabling reverse path check on ICX 7750 devices reduces the following system-max values by 50 percent:

- ip-route
- ip6-route
- ip-route-default-vrf
- ip6-route-default-vrf
- ip-route-vrf
- ip6-route-vrf

NOTE
Disabling reverse path check doubles the system-max values on ICX 7750 devices.

You should configure these values after reloading. You should adjust or remove the max-route configuration in VRFs before reload.

Examples

The following example enables unicast Reverse Path Forwarding globally.

```
device(config)# reverse-path-check
```

History

Release version	Command history
08.0.30	This command was introduced.

ring-interface

Configures the primary and secondary interfaces for the ring to control outward traffic flow.

Syntax

ring-interface ethernet *stackid/slot/port* **ethernet** *stackid/slot/port*

no ring-interface ethernet *stackid/slot/port* **ethernet** *stackid/slot/port*

Command Default

The primary and secondary interfaces are not configured.

Parameters

ethernet *stackid/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.

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 1/1/1 ethernet 1/1/2
```

rmon alarm

Configures an RMON alarm.

Syntax

rmon alarm *alarm-num mib-object sample-interval* { **absolute** | **delta** } **falling-threshold** *falling-threshold-value event* **rising-threshold** *rising-threshold-value event* **owner** *alarm-owner*

no rmon alarm *alarm-num mib-object sample-interval* { **absolute** | **delta** } **falling-threshold** *falling-threshold-value event* **rising-threshold** *rising-threshold-value event* **owner** *alarm-owner*

Command Default

RMON alarm is not configured.

Parameters

alarm-num
Specifies the alarm number. The value can range from 1 to 65535.

mib-object
Specifies the MIB object to monitor.

sample-interval
Specifies the sample interval.

asolute
Configures to test each sample directly.

delta
Configures to test the delta between the samples.

falling-threshold
Configures the falling threshold.

falling-threshold-value
Specifies the threshold value. The value can range from 0 to 2147483647.

event
Specifies the event to fire when the falling threshold crosses the configured value. The value can range from 1 through 65535.

rising-threshold
Configures the rising threshold.

rising-threshold-value
Specifies the threshold value. The value can range from 0 to 2147483647.

event
Specifies the event to fire when the rising threshold crosses the configured value. The value can range from 1 through 65535.

owner *alarm-owner*
Specifies the alarm owner.

Modes

Global configuration mode

Usage Guidelines

Alarm is designed to monitor configured thresholds for any SNMP integer, time tick, gauge or counter MIB object. Using the CLI, you can define what MIB objects are monitored, the type of thresholds that are monitored (falling, rising or both), the value of those thresholds, and the sample type (absolute or delta).

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.

You can configure both the falling threshold and the rising threshold and in any order.

The **no** form of the command removes the configured RMON alarm.

Examples

The following example shows how to configure an alarm.

```
device(config)# rmon alarm 1 ifInOctets.6 10 delta rising-threshold 100 1 falling threshold 50 1 owner
nyc02
```

rmon event

Defines the action to be taken when an alarm is reported and collects and stores reported events for retrieval by an RMON application.

Syntax

rmon event *event-entry* **description** *event-description* { { **execute** | **log-and-execute** | **log-trap-and-execute** | **trap-and-execute** } [**argument** *string*] | **log** | **trap** | **log-and-trap**} **owner** *event-owner*

no rmon event *event-entry* **description** *event-description* { { **execute** | **log-and-execute** | **log-trap-and-execute** | **trap-and-execute** } [**argument** *string*] | **log** | **trap** | **log-and-trap**} **owner** *event-owner*

Command Default

RMON event is not configured.

Parameters

event-entry
Specifies the event number.

description *event-description*
Configures the event description.

execute
Executes batch command when the event fires.

log
Generates RMON log when the event fires.

log-and-execute
Generates RMON log and execute batch command when the event fires.

log-and-trap
Generates RMON log and SNMP trap when the event fires.

log-trap-and-execute
Generates RMON log, SNMP trap and execute batch command when the event fires.

trap
Generates SNMP trap when the event fires.

trap-and-execute
Generates SNMP trap and execute batch command when the event fires.

argument *string*
Specifies batch command argument.

owner *event-owner*
Specifies the batch command augment.

Modes

Global configuration mode

Usage Guidelines

There are two elements to the Event Group--the event control table and the event log table.

The event control table defines the action to be taken when an alarm is reported. Defined events can be found by entering the CLI command, show event. The Event Log Table collects and stores reported events for retrieval by an RMON application.

The **no** form of the command removes the configured RMN event.

Examples

The following example shows how to configure an RMON event.

```
device(config)# rmon event 1 description 'testing a longer string' trap public owner nyc02
```

rmon history

Configure an RMON history control.

Syntax

rmon history *entry-number* **interface** { **ethernet** *stackid/slot/port* | **management** *number* } **buckets** *number* **interval** *sampling-interval* **owner** *owner-name*

no rmon history *entry-number* **interface** { **ethernet** *stackid/slot/port* | **management** *number* } **buckets** *number* **interval** *sampling-interval* **owner** *owner-name*

Command Default

All active ports will generate two history control data entries per active Layer 2 Switch port or Layer 3 Switch interface.

Parameters

entry-number
Specifies the history number. The value can range from 1 to 65535.

interface ethernet *stackid/slot/port*
Specifies the Ethernet interface to monitor.

interface management *number*
Specifies the management interface to monitor.

buckets *number*
Specifies the number of buckets. The value can range from 1 to 65535.

interval *sampling-interval*
Specifies the sample interval. The value can range from 1 to 3600.

owner *owner-name*
Specifies the history owner.

Modes

Global configuration mode

Usage Guidelines

An active port is defined as one with a link up. If the link goes down the two entries are automatically deleted.

Two history entries are generated for each device:

- A sampling of statistics every 30 seconds
- A sampling of statistics every 30 minutes

The history data can be accessed and displayed using any of the popular RMON applications.

The **no** form of the command removes the configured RMON history control.

Examples

The following example shows how to configure the RMON history.

```
device(config)# rmon history 1 interface ethernet 1/1/1 buckets 10 interval 10 owner nyc02
```

route-precedence

Configures a table that defines the order (precedence) in which multicast routes are selected from the multicast routing table (mRTM) and unicast routing (uRTM) table.

Syntax

route-precedence { [**mc-non-default** | **none**] | [**mc-default** | **none**] | [**uc-non-default** | **none**] | [**uc-default** | **none**] }

no route-precedence

Command Default

The default route precedence used to select routes is:

1. A non-default multicast route from the mRTM (**mc-non-default**).
2. A default multicast route from the mRTM (**mc-default**).
3. A non-default unicast route from the uRTM (**uc-non-default**).
4. A default unicast route from the uRTM (**uc-non-default**).

Parameters

mc-non-default
Specifies the precedence for the non-default multicast route table (mRTM).

none
Specifies that this type of route is to be ignored. You can specify this option for any of the multicast or unicast route types.

mc-default
Specifies the precedence for the multicast routing table (mRTM).

uc-non-default
Specifies the precedence for the non-default unicast route table (uRTM).

uc-default
Specifies the precedence for the default unicast route table (uRTM).

Modes

Router PIM configuration mode

Usage Guidelines

The order in which you place the keywords determines the route precedence.

The **no** form of this command restores the default route precedence settings.

You must configure four parameters indicating the four different route types. If you want to specify that a particular route type is not used, configure the **none** keyword to fill the precedence table.

Examples

The following example configures a route precedence in which a non-default multicast route has the highest precedence, and a default unicast route has the lowest precedence. The order used to select routes is:

1. A non-default multicast route from the mRTM.
2. A non-default unicast route from the uRTM.
3. A default multicast route from the mRTM.
4. A default unicast route from the uRTM.

```
device(config)# router pim
device(config-pim-router)# route-precedence mc-non-default uc-non-default mc-default uc-default
```

The following example configures a route precedence in which the unicast default route is ignored. The order used to select routes is:

1. A non-default multicast route from the mRTM.
2. A default multicast route from the mRTM.
3. A non-default unicast route from the uRTM.

```
device(config)# router pim
device(config-pim-router)# route-precedence mc-non-default mc-default uc-non-default none
```

History

Release version	Command history
8.0.10a	This command was introduced.

route-precedence admin-distance

Configures route precedence so that multicast routes are selected from the best route in the multicast routing table (mRTM) and unicast routing (uRTM) table.

Syntax

route-precedence admin-distance

no route-precedence admin-distance

Command Default

Multicast routes are not selected from the best route in the mRTM and uRTM. Routes are selected based on:

- The route precedence configured using the **route-precedence** command.
- The system route precedence default (if route precedence has not been configured using the **route-precedence** command.

the default route precedence settings.

Modes

PIM configuration mode

Usage Guidelines

The **no** form of this command restores the previous route precedence settings.

If the mRTM and the uRTM have routes of equal cost, the route from the mRTM is preferred.

Examples

The following example configures route precedence so that the best multicast route from the mRTM and uRTM tables is selected.

```
Device(config)#router pim
Device(config-pim-router)#route-precedence admin-distance
```

History

Release version	Command history
8.0.10a	This command was introduced.

router bgp

Enables BGP routing.

Syntax

router bgp

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable BGP routing.

Examples

This example enables BGP routing.

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

router-interface

Attaches a router interface to a Layer 2 VLAN.

Syntax

router-interface ve *num*

no router-interface ve *num*

Command Default

A router interface is not configured.

Parameters

ve *num*

Specifies a virtual router interface number.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command removes the router interface from the VLAN.

Examples

The following example shows how to attach the router interface to a Layer 2 VLAN.

```
device(config)# vlan 1 by port
device(config-vlan-1)# untagged ethernet 1/1/1
device(config-vlan-1)# tagged ethernet 1/1/8
device(config-vlan-1)# router-interface ve 1
```

router msdp

Enables multicast source discovery protocol (MSDP) on a router.

Syntax

router msdp [**vrf** *vrf-name*]

Command Default

MSDP is not enabled.

Parameters

vrf *vrf-name*

Specifies a virtual routing and forwarding (VRF) instance.

Modes

Global configuration mode

Usage Guidelines

When you configure the **no router msdp vrf** *vrf-name* command, the MSDP configuration is removed only from the specified VRF.

The PIM Sparse Rendezvous Point (RP) is also an MSDP peer.

Devices that run MSDP usually also run BGP. The source address used by the MSDP device is normally configured to be the same source address used by BGP.

All MSDP parameters available for the default router instance are configurable for a VRF-based MSDP instance.

Examples

The following example enables MSDP.

```
Device(config)# router msdp
```

The following example enables MSDP on a VRF named blue.

```
Device(config)# router msdp vrf blue
```

The following example removes the MSDP configuration only from the VRF named blue.

```
Device(config-msdp-router-vrf-blue)# no router msdp vrf blue
```

route-only

Enables Brocade Layer 3 switches to support Layer 2 switching.

Syntax

route-only

no route-only

Command Default

By default, Brocade Layer 3 switches support Layer 2 switching.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

By default, Brocade Layer 3 switches support Layer 2 switching. These devices modify the routing protocols that are not supported on the devices. If you want to disable Layer 2 switching, you can do so globally or on individual ports, depending on the version of software your device is running.

Enabling or disabling Layer 2 switching is supported in Layer 3 software images only. Enabling or disabling Layer 2 switching is not supported on virtual interfaces.

Brocade FCX 6430, FCX 6450, FCX 6430-C12, ICX 6450, and ICX 6610 devices support both the ingress and egress L2 traffic suppression on a route-only port.

Brocade ICX 7750, ICX 7450, ICX 7250, and ICX 7150 devices support only ingress L2 traffic suppression on a route-only port.

The **no** form of the command enables Layer 2 switching on a Layer 3 switch.

To disable Layer 2 switching only on a specific interface, go to the interface configuration level for that interface, and then configure the command.

Examples

The following example globally disables Layer 2 switching on a Layer 3 switch.

```
device(config)# route-only
device(config)# exit
device# write memory
device# reload
```

The following example enables Layer 2 switching on a Layer 3 switch.

```
device(config)# no route-only
device(config)# exit
device# write memory
device# reload
```

The following example disables Layer 2 switching on Ethernet interface 1/1/1.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# route-only
device(config-if-e1000-1/1/1)# end
device# write memory
device# reload
```

router pim

Configures basic global protocol-independent multicast (PIM) Sparse parameters on a device within the PIM Sparse domain and enters PIM-router configuration mode.

Syntax

router pim [**vrf** *vrf-name*]

no router pim [**vrf** *vrf-name*]

Command Default

PIM Sparse is not configured.

Parameters

vrf *vrf-name*

Specifies a virtual routing and forwarding (VRF) instance.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **no** form of this command disables PIM and removes all configuration for PIM multicast on the device (**router pim** level) only.

Configuring the **no router pim vrf** *vrf-name* command removes all configuration for PIM multicast on the specified VRF.

You do not need to globally enable IP multicast routing when configuring PIM Sparse.

After you enable IP multicast routing and PIM Sparse at the global level, you must enable it on the individual interfaces connected to the PIM Sparse network.

If you configure PIM Sparse on an interface that is on the border of the PIM Sparse domain, you also must also configure the **ip pim border** command on the interface.

You must configure the **bsr-candidate ethernet** command to identify an interface on at least one device as a candidate PIM Sparse Bootstrap router (BSR) and candidate PIM Sparse Rendezvous Point (RP).

You can configure the **rp-address** command to explicitly identify an RP, including an ACL-based RP, by its IP address instead of having it identified by the RP election process.

Entering the **router pim vrf** command to enable PIM does not require a software reload.

All PIM parameters available for the default router instance are configurable for a VRF-based PIM instance.

Examples

This example configures basic global PIM Sparse parameters.

```
device(config)# router pim
```

This example configures PIM Sparse on a VRF named blue.

```
device(config)# router pim blue
```

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
```

rpf-mode

Enables strict or loose unicast Reverse Path Forwarding (uRPF) modes on ICX 7750 devices.

Syntax

rpf-mode [**strict** | **loose**] [**urpf-exclude-default**]

no rpf-mode [**strict** | **loose**] [**urpf-exclude-default**]

Command Default

uRPF mode is not enabled.

Parameters

strict

Specifies uRPF strict mode.

loose

Specifies uRPF loose mode. This mode allows all packets to pass the uRPF check.

urpf-exclude-default

Excludes the default route for uRPF source IP lookup.

Modes

Interface configuration mode

Usage Guidelines

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

You must enable uRPF at the global level before enabling the mode (strict or loose). This command is applicable only to the Layer 3 physical interface and Layer 3 VE interfaces.

The **loose** option allows all packets to pass through. Choose the **loose**mode along with the **urp-exclude-default** option to subject the packets to uRPF check.

Examples

The following example sets the Reverse Path Forwarding mode to strict mode.

```
device(config)# interface ethernet 1/1/3
device(config-if-e1/1/3)# rpf-mode strict
```

History

Release version	Command history
08.0.30	This command was introduced.

rp-address

Configures a device interface as a rendezvous point (RP).

Syntax

rp-address { *ip-address* | *ipv6-address* } *acl_name_or_id*

no rp-address { *ip-address* | *ipv6-address* }

Command Default

The RP is selected by the PIM Sparse protocol's RP election process.

Parameters

ip-address
: Specifies the IP address of the RP.

ipv6-address
: Specifies the IPv6 address of the RP.

acl_name_or_id
: Specifies the name or ID of the ACL that specifies which multicast groups use the RP.

Modes

Router PIM configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of this command restores the default and the RP is selected by the RP election process.

Devices in the PIM Sparse domain use the specified RP and ignore group-to-RP mappings received from the bootstrap router (BSR).

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the BSR sends to each of the PIM Sparse routers.

NOTE
Specify the same IP or IPv6 address as the RP on all PIM Sparse devices within the PIM Sparse domain. Make sure the device is on the backbone or is otherwise well connected to the rest of the network.

Examples

This example configures the device interface at IP address 207.95.7.1 as the RP for the PIM Sparse domain.

```
device(config)# router pim
device(config-pim-router)# rp-address 207.95.7.1
```

This example configures an ACL named acl1 to specify which multicast groups use the RP.

```
device(config)# router pim
device(config-pim-router)# rp-address 130.1.1.1 acl1
```

This example configures an RP for a VRF named blue.

```
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# rp-address 31::207
```

rp-adv-interval

Configures the interval at which the candidate rendezvous point (RP) configured on the device sends candidate-RP advertisement messages to the bootstrap router (BSR).

Syntax

rp-adv-interval *seconds*

no rp-adv-interval *seconds*

Command Default

The device sends candidate-RP advertisement messages every 60 seconds.

Parameters

seconds

Specifies the interval, in seconds, between advertisement messages. The range is 10 through 65535 seconds. The default is 60 seconds.

Modes

PIM router configuration mode

PIM router VRF configuration mode

Usage Guidelines

The **no** form of this command restores the candidate-RP advertisement-message interval to 60 seconds.

Examples

The following example configures the candidate-RP advertisement-message interval to 90 seconds.

```
Device(config)#router pim
Device(config-pim-router)#rp-adv-interval 90
```

The following example configures, on a VRF named blue, the candidate-RP advertisement-message interval to 90 seconds.

```
Device(config)#ipv6 router pim vrf blue
Device(config-ipv6-pim-router-vrf-blue)#rp-adv-interval 90
```

rp-candidate

Configures a device as a candidate rendezvous point (RP) for all multicast groups with the prefix 224.0.0.0/4, by default, and explicitly adds or deletes groups with other prefixes.

Syntax

rp-candidate { **ethernet** *stackid* / *slot* / *portnum* | **loopback** *num* | **ve** *num* | **tunnel** *num* }

rp-candidate {**add** | **delete** } *group-addr mask-bits*

no rp-candidate { **ethernet** *stackid* / *slot* / *portnum* | **loopback** *num* | **ve** *num* | **tunnel** *num* }

no rp-candidate {**add** | **delete** } *group-addr mask-bits*

Command Default

The PIM router is not available for selection as an RP.

Parameters

ethernet *stackid/slot/portnum*
: Specifies a physical interface for the candidate RP. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *num*
: Specifies a loopback interface for the candidate RP.

ve *num*
: Specifies a virtual interface for the candidate RP.

tunnel *num*
: Specifies a GRE tunnel interface for the candidate RP.

add
: Specifies adding a group address or range of group addresses to the default group configured by the those the device is the candidate RP for by default, that is, groups with the prefix 224.0.0.0/4.

delete
: Specifies deleting a group address or range of group addresses, that were added using the **add** keyword.

group-addr mask-bits
: Specifies the group address and the number of significant bits in the subnet mask.

Modes

Router PIM configuration mode

Usage Guidelines

The **no rp-candidate** command makes the PIM router cease to act as a candidate RP.

The **no rp-candidate add** command deletes a group address or range of group addresses that were added using the **add** keyword.

Configuring the **rp-candidate** command on an Ethernet, loopback, virtual, or tunnel interface, configures the device as a candidate RP for all multicast groups with the prefix 224.0.0.0/4, by default. You can configure the **rp-candidate add** command to add to those a group address or range of group addresses. You can configure the **rp-candidate delete** command to delete a group address or range of group addresses that were added to the default addresses.

NOTE
You cannot delete the default group prefix.

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the bootstrap router (BSR) sends to each of the PIM Sparse routers.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

NOTE
Specify the same IPv6 address as the RP on all IPv6 PIM Sparse routers within the IPv6 PIM Sparse domain. Make sure the device is on the backbone or is otherwise well connected to the rest of the network. You can configure the **rp-address** command to specify the RP address.

Examples

This example configures a physical device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate ethernet 1/2/2
```

This example uses a loopback interface to configure a device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate loopback 1
```

This example uses a virtual interface to configure a device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate ve 120
```

This example configures an address group to the devices for which it is a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate add 224.126.0.0 16
```

This example deletes an address group from the devices for which it is a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate delete 224.126.22.0 24
```

History

Release version	Command history
8.0.20	This command was modified to add the **tunnel** keyword.

save-current-values

Configures a backup to save the VSRP timer values received from the master instead of the timer values configured on the backup.

Syntax

save-current-values

no save-current-values

Command Default

By default, the backups always use the value of the timers received from the master.

Modes

VSRP VRID configuration mode

Usage Guidelines

Saving the current timer values instead of the configured ones helps ensure consistent timer usage for all the VRID devices.

The **no** form of the command disables saving the timer values from the master.

Examples

The following example shows how to configure a backup to save the VSRP timer values received from the master instead of the timer values configured on the backup.

```
device(config)# vlan 200
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# save-current-values
```

save-dynamicvlan-to-config

Configures the Brocade device to save the RADIUS-specified VLAN assignments to the running-config file of the device.

Syntax

save-dynamicvlan-to-config

no save-dynamicvlan-to-config

Command Default

The dynamic VLAN assignments are not saved to the running-config file.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command ensures that the RADIUS-specified VLAN assignments are not saved to the running-config file of the device.

Examples

The following example configures the device to save the RADIUS-specified VLAN assignments to the running-config file of the device.

```
device(config)# dot1x-enable
device(config-dot1x)# save-dynamicvlan-to-config
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

server (NTP)

Configures the device in client mode and specifies the NTP servers to synchronize the system clock.

Syntax

server { *ipv4-address* | *ipv6-address* } [**version** *version-number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**burst**]

no server { *ipv4-address* | *ipv6-address* } [**version** *version-number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**burst**]

Parameters

ipv4-address
: Specifies the IP address of the server providing the clock synchronization.

ipv6-address
: Specifies the IPv6 address of the server providing the clock synchronization.

version *version-number*
: Specifies the Network Time Protocol (NTP) version number. Valid values are 3 or 4. The default value is 4.

key *key-id*
: Specifies the authentication key range. The value can range from 1 to 65535.

minpoll *interval*
: Specifies the shortest polling interval. The range is from 4 through 17. Default is 6. The interval argument is power of 2 (4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s, and so on).

maxpoll *interval*
: Specifies the longest polling interval. The range is from 4 through 17. Default is 10. The interval argument is calculated by the power of 2 (4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s, and so on).

burst
: Sends a burst of packets to the server at each polling interval.

Modes

NTP configuration mode

Usage Guidelines

A maximum 8 NTP servers can be configured.

The **no** form of the command removes the NTP server configuration.

Examples

The following example shows how to configure the NTP server.

```
device(config)# ntp
device(config-ntp)# server 1.1.1.1 key 23 maxpoll 15 minpoll 8 version 3 burst
```

servertimeout

Configures the amount of time the Brocade device should wait for the RADIUS server to respond to the message before retransmitting the message.

Syntax

servertimeout *seconds*

no servertimeout *seconds*

Command Default

The default value is 30 seconds.

Parameters

seconds

Specifies the amount of time the Brocade device should wait for the RADIUS server to respond to the message before retransmitting the message. The value range is from 1 through 4294967295. The default value is 30 seconds.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command resets the default time of 30 seconds for the Brocade device to wait for the RADIUS server to respond to the message before retransmitting the message.

Examples

The following example configures the device to retransmit a message if the RADIUS server does not respond to its message within 45 seconds.

```
device(config)# dot1x-enable
device(config-dot1x)# servertimeout 45
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

scale-timer

Changes the timer scale.

Syntax

scale-timer *number*

no scale-timer *number*

Command Default

By default, the timer scale is set to 1.

Parameters

number

Specifies the multiplier factor for the timer. The range for the timer is from 1 through 10.

Modes

Global configuration mode

Usage Guidelines

To achieve sub-second failover times, you can shorten the duration of all scale timers for VSRP, VRRP, and VRRP-E by adjusting the timer scale. The timer scale is a value used by the software to calculate the timers. If you increase the timer scale, each timer value is divided by the scale value. Using the timer scale to adjust timer values enables you to easily change all the timers while preserving the ratios among their values. For example, if you set the timer scale to 2, all VSRP, VRRP, and VRRP-E timer values will be divided by 2.

The **no** form of the command sets the multiplier to 1.

Examples

The following example shows how to set the scale timer to 2.

```
device(config)# scale-timer 2
```

scheduler-profile

Attaches a scheduler profile to one or more ports.

Syntax

scheduler-profile *profile-name*

no scheduler-profile *profile-name*

Command Default

A scheduler profile is not attached to a port.

Parameters

profile-name

Specifies the name of the scheduler profile to be attached to the port.

Modes

Interface mode

Multiple-interface mode

Usage Guidelines

The **no** form of this command removes the scheduler profile from the port or ports.

You must configure a user scheduler profile before you can attach it to a port.

Only one scheduler profile at a time can be attached to any port. You can attach a scheduler profile to more than one port.

Examples

The following example attaches a scheduler profile named user1 to a port.

```
Device(config-if-e10000-1/1/1)# scheduler-profile user1
```

The following example attaches a scheduler profile named user2 to multiple ports.

```
Device(config-mif-1/1/2-1/1/16)# scheduler-profile user2
```

The following example removes a scheduler profile named user2 from multiple ports.

```
Device(config-mif-1/1/2-1/1/16)# no scheduler-profile user2
```

History

Release version	Command history
8.0.10	This command was introduced.

set-active-mgmt

Sets the active management slot.

Syntax

set-active-mgmt *mgmt-slot-number*

Command Default

The default active management preference is set to mgmt0 (slot 9).

Parameters

mgmt-slot-number

Specifies the active management slot number. The valid values are mgmt0 and mgmt1.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on FSX devices.

A management slot which is in active management preference will always attempt to be active on the next reboot.

Examples

The following example show how set the active management slot number to slot 10.

```
device(config)# set-active-mgmt mgmt1
```

set ip next-hop

Configures the next-hop IP address for the traffic that matches a match statement in the route map.

Syntax

set ip next-hop { **peer-address** | *ip-address* [**no-ttl-decrement**] }

no set ip next-hop { **peer-address** | *ip-address* [**no-ttl-decrement**] }

Command Default

The next-hop IP address is not configured by default.

Parameters

peer-address

Specifies the BGP peer IP address.

ip-address

Specifies the IP address of the next hop.

no-ttl-decrement

Disables the TTL value decrement and ensures that the packets are forwarded to the neighbor router without decrementing Time-to-Live (TTL) for the matched traffic.

Modes

Route map configuration mode

Usage Guidelines

no-ttl-decrement

Policy-based Routing (PBR) does not support **peer-address** option while configuring the next-hop IP address using the **set ip next-hop** command.

The **no-ttl-decrement** option is supported only on the Brocade ICX 7750 and Brocade ICX 7450 devices.

The **no** form of the command removes the next-hop IP address configured for the traffic.

Examples

The following example configures a route map without decrementing the Time-to-Live (TTL) value.

```
device(config)# route-map test-route permit 99
device(config-routemap test-route)# match ip address 100
device(config-routemap test-route)# set ip next-hop 192.168.3.1 no-ttl-decrement
device(config-routemap test-route)# exit
```

History

Release version	Command history
08.0.10d	The **no-ttl-decrement** option was introduced.
08.0.30	The support for the **no-ttl-decrement** option was added in 08.0.30 and later releases.

sflow agent-ip

Configures an arbitrary IPv4 or IPv6 address as the sFlow agent IP address.

Syntax

sflow agent-ip { *ipv4-addr* | *ipv6-addr* }

no sflow agent-ip { *ipv4-addr* | *ipv6-addr* }

Command Default

By default, the device automatically selects the sFlow agent IP address based on the configuration.

Parameters

ipv4-addr

Specifies the IPv4 address as the sFlow agent IP address.

ipv6-addr

Specifies the IPv6 address as the sFlow agent IPv6 address.

Modes

Global configuration mode

Usage Guidelines

The sampled sFlow data sent to the collectors includes an agent_address field. This field identifies the device (the sFlow agent) that sent the data. By default, the device automatically selects the sFlow agent IP address based on the configuration. Alternatively, you can configure the device to instead use an arbitrary IPv4 or IPv6 address as the sFlow agent IP address.

The **no** form of the command removes the configured IPv4 or IPv6 address as the sFlow agent IP address.

Examples

The following example shows how to configure an IPv4 address as the sFlow agent IP address.

```
device(config)# sflow agent-ip 10.10.10.1
```

The following example shows how to configure an IPv6 address as the sFlow agent IP address.

```
device(config)# sflow agent-ip FE80::240:D0FF:FE48:4672
```

sflow destination

Configures an sFlow collector.

Syntax

sflow destination [*ipaddress* | **ipv6** *ipv6-address*] [*udp-port-number*] [**vrf** *vrf-name*]

no sflow destination [*ipaddress* | **ipv6** *ipv6-address*] [*udp-port-number*] [**vrf** *vrf-name*]

Command Default

sFlow collector is not configured.

Parameters

ipaddress
: Specifies the IPv4 destination address.

ipv6 *ipv6-address*
: Specifies the IPv6 destination address.

udp-port-number
: Specifies the udp port number. The default value is 6343.

vrf *vrf-name*
: Specifies the VRF name.

Modes

Global configuration mode

Usage Guidelines

sFlow exports traffic statistics to an external collector. You can specify up to four collectors. You can specify more than one collector with the same IP address if the UDP port numbers are unique. You can have up to four unique combinations of IP addresses and UDP port numbers.

By default sFlow uses the management VRF to send the samples to the collector. If no management VRF is configured, sFlow uses the default VRF, and this default VRF ID will be assigned to any configured collector that does not have a user-included VRF.

sFlow forwarding ports can come from ports belonging to any VRF. The port does not have to be in the same VRF as the collector. sFlow collects packets from all sFlow forwarding ports, even if they do not belong to a VRF, compiles the packets into the sFlow samples, and sends the samples to the particular collector with no filtering for VRF membership.

The **no** form of the command set the management VRF to send the samples to the collector.

Examples

The following example shows how to configure a sFlow collector and specify a VRF.

```
device(config)#  sflow destination 10.10.10.10 vrf customer1
```

sflow enable

Enables sFlow forwarding globally.

Syntax

sflow enable

no sflow enable

Command Default

sFlow is not enabled.

Modes

Global configuration mode

Usage Guidelines

To enable sFlow forwarding, you must first enable it on a global basis, then use the **sflow forwarding** command to enable it on individual interfaces or LAG ports, or both.

The **no** form of the command disables sFlow forwarding globally.

Examples

The following example shows how to enable sFlow forwarding globally.

```
device(config)# sflow enable
```

sflow export

Configures exporting of the CPU and memory usage information or exporting CPU-directed data to the sFlow collector.

Syntax

sflow export { **cpu-traffic** [*traffic-seconds*] | **system-info** [*info-seconds*] }

no sflow export system-info { **cpu-traffic** [*traffic-seconds*] | **system-info** [*info-seconds*] }

Command Default

By default, CPU usage information and memory usage information or CPU-directed data are not exported.

The default polling interval for exporting CPU and memory usage information to the sFlow collector is 20 seconds and the interval for exporting CPU-directed data to the sFlow collector is 16.

Parameters

traffic-seconds

Specifies the average ratio of the number of incoming packets on an sFlow-enabled port, to the number of flow samples taken from those packets.

info-seconds

Specifies the polling interval.

Modes

Global configuration mode

Usage Guidelines

The polling interval defines how often sFlow data for a port is sent to the sFlow collector.

The **no** form of the command removes the configured value and sets the sampling rate or the polling interval to its default value.

Examples

The following example shows how to set the sampling rate to 2048.

```
device(config)# sflow export cpu-traffic 2048
```

The following example shows how to enable the export of CPU usage and memory usage information.

```
device(config)# sflow export system-info
```

The following example shows how to set the polling interval for exporting CPU and memory usage information to 30 seconds.

```
device(config)# sflow export system-info 30
```

sflow forwarding

Enables sFlow forwarding on individual interfaces.

Syntax

sflow forwarding

no sflow forwarding

Command Default

sFlow forwarding is not enabled on individual interfaces.

Modes

Interface configuration mode

Usage Guidelines

You must use both the **sflow enable** and **sflow forwarding** commands to enable the feature.

The **no** form of the command disables sFlow forwarding on individual interfaces.

Examples

The following example shows how to enable sFlow forwarding on interfaces.

```
device(config)# sflow enable
device(config)# interface ethernet 1/1/1 to 1/1/8
device(config-mif-1/1/1-1/1/8)# sflow forwarding
```

sflow forwarding (LAG)

Enables sFlow forwarding on an individual port in a deployed LAG.

Syntax

sflow forwarding { **ethernet** *stackid/slot/port* | **port-name** *name* }

no sflow forwarding { **ethernet** *stackid/slot/port* | **port-name** *name* }

Command Default

sFlow is not configured.

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet port within the LAG on which you want to enable sFlow forwarding.

port-name *name*

Specifies a named port within the LAG on which you want to enable sFlow forwarding.

Modes

LAG configuration mode

Usage Guidelines

For a keep-alive LAG, sFlow can be enabled only in interface configuration mode and not in LAG configuration mode.

The **no** form of the command disables sFlow forwarding.

Examples

The following example shows how to enable sFlow forwarding on an individual port.

```
device(config)# lag blue static
device(config-lag-blue)# deploy
device(config-lag-blue)# sflow forwarding ethernet 1/3/1
```

The following example shows how to enable sFlow forwarding on a named port.

```
device(config)# lag test2 static
device (config-lag-test2)# deploy
device(config-lag-test2)# sflow forwarding port-name port1
```

sflow management-vrf-disable

Disables the management VRF in sFlow.

Syntax

sflow management-vrf-disable

no sflow management-vrf-disable

Command Default

sFlow uses the management VRF to send the samples to the collector.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command enables the management VRF in sFlow.

Examples

The following example shows how to disable management VRF in sFlow.

```
device(config)# sflow management-vrf-disable
```

sflow max-packet-size

Configures the maximum flow samples sent to the sFlow collector.

Syntax

sflow max-packet-size *size*

no sflow max-packet-size *size*

Command Default

The default maximum flow sample size is 128 bytes.

Parameters

size

Specifies the max sflow packet size. For sFlow version 5, the maximum flow sample size is 1300 bytes.

Modes

Global configuration mode

Usage Guidelines

With sFlow version 5, you can specify the maximum size of the flow sample sent to the sFlow collector. If a packet is larger than the specified maximum size, then only the contents of the packet up to the specified maximum number of bytes is exported. If the size of the packet is smaller than the specified maximum, then the entire packet is exported.

The **no** form of the command removes the configured value and reverts to the default value.

Examples

The following example shows how to set the maximum flow sample size to 1024.

```
device(config)# sflow max-packet-size 1024
```

sflow polling-interval

Configures the sflow polling interval.

Syntax

sflow polling-interval *secs*

no sflow polling-interval [*secs*]

Command Default

The default polling interval is 20 seconds.

Parameters

secs

Specifies the polling interval. The value can range from 0 through 429496729 seconds. If you specify 0, counter data sampling is disabled. The default polling interval is 20 seconds.

Modes

Global configuration mode

Usage Guidelines

The polling interval defines how often sFlow byte and packet counter data for a port are sent to the sFlow collectors. If multiple ports are enabled for sFlow, the device staggers transmission of the counter data to smooth performance. For example, if sFlow is enabled on two ports and the polling interval is 20 seconds, the device sends counter data every ten seconds. The counter data for one of the ports are sent after ten seconds, and counter data for the other port are sent after an additional ten seconds. Ten seconds later, new counter data for the first port are sent.

The interval value applies to all interfaces on which sFlow is enabled.

The **no** form of the command returns the polling interval to the default value.

Examples

The following example shows how to set the polling interval to 30 seconds.

```
device(config)# sflow polling-interval 30
```

sflow sample

Changes the default sampling rate.

Syntax

sflow sample *num*

no sflow sample *num*

Command Default

The default sampling rate is 4096 packets.

Parameters

num

Specifies the average number of packets from which each sample is taken. The software rounds the value that you enter to the next higher odd power of 2. Refer to the Usage Guidelines section for information on the range of supported values.

Modes

Global configuration mode

Interface configuration mode

LAG configuration mode

Usage Guidelines

The value range for the sampling rate on Brocade ICX 7250, ICX 7450, and ICX 7750 is from 256 through 1073741823.

You cannot change a module's sampling rate directly. You can change a module's sampling rate only by changing the sampling rate of a port on that module.

You can configure an individual port to use a different sampling rate than the global default sampling rate. This is useful when ports have different bandwidths.

You can configure individual LAG ports to use a different sampling rate than the global default sampling rate. Configuring a sampling rate on a port that is the primary port of a LAG applies that same sampling rate to all ports in the LAG. For a keep-alive LAG, sFlow can be enabled only at the interface level and not at the LAG level.

When configuring the sample rate, if you configure the value as 1000, the software rounds the value to the next higher odd power of 2; so the actual rate is 2^11 (2048), and 1 in 2048 packets are sampled by the hardware.

The **no** form of the command resets the sampling rate to the default value.

Examples

The following example changes the default (global) sampling rate.

```
device(config)# sflow sample 2048
```

The following example changes the sampling rate on an individual port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# sflow sample 8192
```

The following example enables an sFlow sample rate in a LAG configuration.

```
device(config)# lag blue static
device(config-lag-blue)# deploy
device(config-lag-blue)# sflow sample 512
```

sflow sample-mode

Enables sample mode so that dropped packets are included in sFlow sampling.

Syntax

sflow sample-mode all

no sflow sample-mode all

Command Default

Sample mode is not enabled. Dropped packets are not included in sFlow sampling.

Parameters

all

Specifies that all packets (non-dropped and dropped) are included in sFlow sampling.

Modes

Global configuration mode

Usage Guidelines

The **sflow sample-mode** command is not supported on ICX 7750, ICX 7450, ICX 7250, ICX 6430, ICX 6650, and FSX 800/1600 devices.

The **no** form of the command restores the default behavior and only the non-dropped packets are included in sFlow sampling.

Examples

The following example configures the sFlow sample mode to include all packets.

```
device(config)# sflow sample-mode all
```

History

Release version	Command history
08.0.30	This command was introduced.

sflow source

Configures the sFlow source interface (IPv4 or IPv6) from which the IP source address is selected for the sFlow datagram.

Syntax

sflow source [**ipv6**] { **ethernet** *stackid/slot/port* | **ve** *ve-number* | **loopback** *number* }

no sflow source [**ipv6**] { **ethernet** *stackid/slot/port* | **ve** *ve-number* | **loopback** *number* }

Command Default

The sFlow source is not configured. The IP address of the outgoing interface is used in the sFlow datagram.

Parameters

ipv6

Configures the IPv6 interface as the sFlow source. If **ipv6** is not specified, the IPv4 interface is automatically configured as the sFlow source.

ethernet *stackid/slot/port*

Configures an Ethernet interface as the sFlow source interface.

ve *ve-number*

Configures a virtual interface (VE) as the sFlow source interface.

loopback *number*

Configures a loopback interface as the sFlow source interface.

Modes

Global configuration mode

Usage Guidelines

At any time, only one source of the Ethernet, VE, or loopback interface can be specified as the source interface.

The first IP address in the interface IP address list is considered the source IP address. Upon configuring another source for an IPv4 or IPv6 address, any previously configured source for the IPv4 or IPv6 address will be deleted. You can configure IPv4 and IPv6 source interfaces independently.

If the sFlow destination is IPv6, and the sFlow source is configured for an IPv6 address, then an IPv6 address will be selected from the configured interface. If the sFlow destination is IPv4, and the sFlow source is configured for an IPv4 address, then an IPv4 address will be selected from the configured interface.

The **no** form of the command removes the sFlow source configuration from the interface and restores the default behavior of using IP address of the outgoing interface as the source IP address of the sFlow datagram.

Examples

The following example configures an Ethernet interface to be used as the sFlow source IPv6 interface.

```
device(config)# sflow source ipv6 ethernet 1/1/2
```

The following example configures an Ethernet interface to be used as the sFlow source IPv4 interface.

```
device(config)# sflow source ethernet 1/1/3
```

History

Release version	Command history
08.0.30	This command was introduced.

sflow source-port

Configures the source UDP port.

Syntax

sflow source-port *num*

no sflow source-port *num*

Command Default

sFlow sends data to the collector using UDP source port 8888.

Parameters

num

Specifies the sFlow source port. The value can range from 1025 to 65535.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command reverts the sFlow source port to its default port 8888.

Examples

The following example shows how to change the source UDP port to 8000.

```
device(config)# sflow source-port 8000
```

sflow version

Configures the version used for exporting sFlow data.

Syntax

sflow version *version-num*

no sflow version [*version-num*]

Command Default

When sFlow is enabled globally on the device, the sFlow agent exports sFlow data in version 5 format.

Parameters

version-num

Specifies the version number. The version can be 2 or 5.

Modes

Global configuration mode

Usage Guidelines

You can switch between versions without rebooting the device or disabling sFlow.

NOTE
When the sFlow version number is changed, the system will reset sFlow counters and flow sample sequence numbers.

The **no** form of the command resets the sFlow verison to its default.

Examples

The following example shows how to set the sFlow version to 2.

```
device(config)# sflow version 2
```

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

Virtual-router-group 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 **no short-path-forwarding** to remove this configuration.

Examples

To enable short-path-forwarding on a VRRP-E group:

```
device# configure terminal
device(config)# router vrrp-extended
switch(config-vrrpe-router)# slow-start 40
switch(config-vrrp-extended-group-100)# short-path-forwarding
```

Show Commands

show 802-1w

Displays the Rapid Spanning Tree Protocol (RSTP) information of the specified port-based VLAN.

Syntax

show 802-1w [**detail**] [*number* | **vlan** *vlan-id*]

Parameters

detail

Displays detailed output.

number

Specifies the number of spanning tree entries to skip before the display begins.

vlan *vlan-id*

Displays the RSTP details for a specific VLAN.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

VLAN configuration mode

Examples

The following example shows the output of the **show 802-1w** command.

```
device# show 802-1w
--- VLAN 4 [ STP Instance owned by VLAN 4 ] ----------------------------
Bridge IEEE 802.1W Parameters:
Bridge             Bridge     Bridge    Bridge     Force       tx
Identifier         MaxAge     Hello     FwdDly     Version     Hold
hex                sec        sec       sec                                                    cnt
8000002022227700   20         2         15         Default    3
RootBridge         RootPath      DesignatedBri-    Root    Max    Fwd   Hel
Identifier         Cost          dge Identifier    Port    Age    Dly   lo
hex
hex                                              sec    sec   sec
8000002022227700   0             8000002022227700  Root    20     15    2
Port IEEE 802.1W Parameters:
<--- Config Params --><-------------- Current state ----------------->
Port    Pri    PortPath    P2P     Edge      Role       State       Designa-     Designated
Num            Cost        Mac     Port                             ted cost     bridge
1/1/1   128    20000       F       F         DESIGNATED FORWARDING  0            8000002022227700
--- VLAN 5 [ STP Instance owned by VLAN 5 ] ----------------------------
Bridge IEEE 802.1W Parameters:
Bridge           Bridge     Bridge       Bridge     Force       tx
Identifier       MaxAge     Hello        FwdDly     Version     Hold
hex              sec        sec          sec                    cnt
8000002022227700 20         2            15         Default     3
RootBridge       RootPath       DesignatedBri-      Root    Max   Fwd   Hel
Identifier       Cost           dge Identifier      Port    Age   Dly   lo
hex                             hex                        sec   sec   sec
8000002022227700 0             8000002022227700    Root    20    15    2
Port IEEE 802.1W Parameters:
<--- Config Params --><-------------- Current state ----------------->
Port     Pri    PortPath    P2P    Edge       Role        State       Designa-      Designated
Num            Cost        Mac    Port                               ted cost      bridge
1/1/1    128    20000       F      F          DESIGNATED  FORWARDING  0             8000002022227700
--- VLAN 6 [ STP Instance owned by VLAN 6 ] ----------------------------
Bridge IEEE 802.1W Parameters:
Bridge           Bridge     Bridge        Bridge     Force        tx
Identifier       MaxAge     Hello         FwdDly     Version      Hold
hex              sec        sec           sec                     cnt
8000002022227700 20         2             15         Default      3
RootBridge       RootPath     DesignatedBri-     Root       Max   Fwd   Hel
Identifier       Cost         dge Identifier     Port       Age   Dly   lo
hex                           hex                           sec   sec   sec
8000002022227700 0            8000002022227700   Root       20    15    2
Port IEEE 802.1W Parameters:
<--- Config Params --><-------------- Current state ----------------->
Port   Pri     PortPath    P2P     Edge       Role        State       Designa-       Designated
Num            Cost        Mac     Port                               ted cost       bridge
1/1/1  128     20000       F       F          DESIGNATED  FORWARDING  0              8000002022227700
```

show aaa

Displays information about all TACACS+ and RADIUS servers identified on the device.

Syntax

show aaa

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show aaa** command displays the following information:

Output field	Description
Tacacs+ key	The setting configured with the **tacacs-server key** command. At the Super User privilege level, the actual text of the key is displayed. At the other privilege levels, a string of periods (....) is displayed instead of the text.
Tacacs+ retries	The setting configured with the **tacacs-server retransmit** command.
Tacacs+ timeout	The setting configured with the **tacacs-server timeout** command.
Tacacs+ dead-time	The setting configured with the **tacacs-server dead-time** command.
Tacacs+ Server	For each TACACS/TACACS+ server, the IP address, port, and the following statistics are displayed: • opens - Number of times the port was opened for communication with the server • closes - Number of times the port was closed normally • timeouts - Number of times the port was closed due to a timeout • errors - Number of times an error occurred while opening the port • packets in - Number of packets received from the server • packets out - Number of packets sent to the server
connection	The current connection status. This can be "no connection" or "connection active".
Radius key	The setting configured with the **radius-server key** command. At the Super User privilege level, the actual text of the key is displayed. At the other privilege levels, a string of periods (....) is displayed instead of the text.
Radius retries	The setting configured with the **radius-server retransmit** command.
Radius timeout	The setting configured with the **radius-server timeout** command.

Output field	Description
Radius Server	For each RADIUS server, the IP address, and the following statistics are displayed: • Auth Port - RADIUS authentication port number (default 1645) • Acct Port - RADIUS accounting port number (default 1646) • opens - Number of times the port was opened for communication with the server • closes - Number of times the port was closed normally • timeouts - Number of times the port was closed due to a timeout • errors - Number of times an error occurred while opening the port • packets in - Number of packets received from the server • packets out - Number of packets sent to the server
connection	The current connection status. This can be "no connection" or "connection active".

Examples

The following example displays information about all TACACS/TACACS+ and RADIUS servers identified on the device.

```
device(config)# show aaa
Tacacs+ key: foundry
Tacacs+ retries: 1
Tacacs+ timeout: 15 seconds
Tacacs+ Server: 10.95.6.90 Port:49:
            opens=6 closes=3 timeouts=3 errors=0
            packets in=4 packets out=4
no connection
Radius key: networks
Radius retries: 3
Radius timeout: 3 seconds
Radius Server: 10.95.6.90 Auth Port=1645 Acct Port=1646:
            opens=2 closes=1 timeouts=1 errors=0
            packets in=1 packets out=4
no connection
```

show access-list

Displays access-list information.

Syntax

show access-list { *acl-name* | *std-acl-num* | *extd-acl-num* | **all** | **hw-usage** { **on** | **off** } }

Parameters

acl-name
: Displays information about the ACL with the specified name.

std-acl-num
: Displays information about the specified standard ACL. Valid values are from 1 through 99.

extd-acl-num
: Displays information about the specified extended ACL. Valid values are from 100 through 199.

all
: Displays information about all ACLs.

hw-usage
: Displays the hardware usage statistics.

on
: Turns on the display of the rule number needed by hardware when displaying ACL.

off
: Turns off the display of the rule number needed by hardware when displaying ACL.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

The number of configured ACL rules can affect the rate at which hardware resources are used. You can use the **show access-list hw-usage on** command to enable hardware usage statistics, followed by the **show access-list** *std-acl-num* command to determine the hardware usage for an ACL. To gain more hardware resources, you can modify the ACL rule so that it uses less hardware resources.

Command Output

The **show access-list all** command displays the following information:

Output field	Description
Rule cam	Lists the number of CAM entries used by the ACL or entry. The number of CAM entries listed for the ACL itself is the total of the CAM entries used by the ACL entries.
Flows	Lists the number of Layer 4 session table flows in use for the ACL.
Packets	Lists the number of packets and is applicable only to flow-based ACLs.

Examples

The following example shows sample output from the **show access-list all** command.

```
device# show access-list all
Extended IP access list 100 (Total flows: N/A, Total packets: N/A, Total rule cam use: 3)
permit udp host 192.168.2.169 any (Flows: N/A, Packets: N/A, Rule cam use: 1)
permit icmp any any (Flows: N/A, Packets: N/A, Rule cam use: 1)
deny ip any any (Flows: N/A, Packets: N/A, Rule cam use: 1)
```

The following example shows sample output from the **show access-list all** command.

```
device# show access-list all
Standard IP access list 1 (hw usage (if applied on 24GC modules) : 2) (hw usage (if applied on 48GC
modules) : 2)
permit any (hw usage (if applied on 24GC modules) : 1) (hw usage (if applied on 48GC modules) : 1)
Extended IP access list 100 (hw usage (if applied on 24GC modules) : 7) (hw usage (if applied on 48GC
modules) : 7)
deny tcp any range newacct src any (hw usage (if applied on 24GC modules) : 6) (hw usage (if applied on
48GC modules) : 6)
```

The following example enables the hardware usage statistics. Once enabled, output of the show access-list command displays the hardware usage statistics.

```
device# show access-list hw-usage on
device# show access-list 100
Extended IP access list 100 (hw usage : 2)
deny ip any any (hw usage : 1
```

show access-list accounting

Displays the Access Control List (ACL) accounting statistics for IPv4 ACLs, IPv6 ACLs, and Layer 2 MAC filters.

Syntax

show access-list accounting { *interface-type interface-name* **in** | **traffic-policy** [**all** | *name*] }

Parameters

interface-type interface-name

Specifies the ID of the Ethernet or virtual interface. Displays the accounting statistics for ACLs bound to a physical port or displays the statistics for ACLs bound to ports that are members of a virtual routing interface.

in

Displays the statistics of the inbound ACLs.

traffic-policy

Displays traffic policy statistics.

all

Displays the statistics of all traffic policies.

name

Displays the statistics of a specific traffic policy.

Modes

Privileged EXEC mode

Command Output

The **show access-list accounting** command displays the following information. The output displayed gives information about IPv4 ACLs or IPv6 ACLs, or MAC filters based on the configuration of the port or interface. If both IPv4 and IPv6 ACLs are configured on the same port, it gives both IPv4 and IPv6 ACL accounting information appears in a single output.

Output field	Description
IPV4 ACL Accounting Information or IPv6 ACL Accounting Information	Denotes the ACL for which the accounting information was collected.
devNum [#] => ACL: Num	Specifies the device number and the ID of the ACL used.
#	Shows the index of the ACL entry, starting with 0, followed by the permit or deny condition defined for that ACL entry. (The first entry created for an ACL is assigned the index 0. The next one created is indexed as 1, and so on.)
Hit count	Shows the number of hits for each counter.

Examples

The following output shows a virtual interface that has both IPv4 and IPv6 ACLs applied to the same port and has ACL accounting enabled.

```
device# show access-list accounting ve 16 in
IPV4 ACL Accounting Information
devNum[0] => ACL: 10
    0: permit any
     Hit Count:   (1Min)            0   (5Sec)                          0
                  (PktCnt)          0 (ByteCnt)                         0
    ----------------------------------------------------------------------
65535: Implicit Rule deny any any
     Hit Count:   (1Min)            0   (5Sec)                          0
                  (PktCnt)          0 (ByteCnt)                         0
    ----------------------------------------------------------------------

IPV6 ACL Accounting Information
devNum[0] => ACL: v6
    0:  permit ipv6 any any
     Hit Count:   (1Min)             0   (5Sec)                          0
                  (PktCnt)           0  (ByteCnt)                        0
    ----------------------------------------------------------------------
65533: Implicit ND_NA Rule: permit any any
     Hit Count:   (1Min)              0   (5Sec)                          0
                  (PktCnt)            0 (ByteCnt)                         0
    ----------------------------------------------------------------------
65534: Implicit ND_NS Rule: permit any any
     Hit Count:   (1Min)              0   (5Sec)                          0
                  (PktCnt)            0 (ByteCnt)                         0
    ----------------------------------------------------------------------
65535: Implicit Rule: deny any any
     Hit Count:   (1Min)              0   (5Sec)                          0
                  (PktCnt)            0 (ByteCnt)                         0
    ----------------------------------------------------------------------
```

The following output from a FastIron SX device shows the per-port display when the device has **acl-per-port-per-vlan** configured for IPv4 and IPv6 on interface 121, which has ports 3/21 and 3/20.

NOTE

In FastIron SX devices, ACL accounting displays only the Byte counter field, and all other fields display “N/A”.

```
device# show access-list accounting ve 121 in

   IPV4 ACL Accounting Information
   perPort[3/20] => Inbound ACL: 10
    0: permit host 10.10.10.1
     Hit Count:   (1Min)       N/A   (5Sec)                  N/A
                  (PktCnt)     N/A (ByteCnt)                  0
    ---------------------------------------------------------------
65535: Implicit Rule deny any any
     Hit Count:   (1Min)       N/A   (5Sec)                  N/A
                  (PktCnt)     N/A (ByteCnt)                  0
    ---------------------------------------------------------------

IPV6 ACL Accounting Information
perPort[3/20] => Inbound ACL: v6
    0:  permit ipv6 any any
     Hit Count:   (1Min)        N/A   (5Sec)                    N/A
                  (PktCnt)     N/A (ByteCnt)                  0
    ---------------------------------------------------------------
    1:  permit ipv6 1000::/64 2000::/64
     Hit Count:   (1Min)       N/A   (5Sec)                  N/A
                  (PktCnt)     N/A (ByteCnt)                  0
    ---------------------------------------------------------------
65533: Implicit ND_NA Rule: permit any any
     Hit Count:   (1Min)        N/A   (5Sec)                  N/A
                  (PktCnt)      N/A (ByteCnt)                  0
    ---------------------------------------------------------------
65534: Implicit ND_NS Rule: permit any any
     Hit Count:   (1Min)    N/A   (5Sec)                      N/A
                  (PktCnt)  N/A (ByteCnt)                      0
    ---------------------------------------------------------------
65535: Implicit Rule: deny any any
     Hit Count:   (1Min)    N/A   (5Sec)                      N/A
                  (PktCnt)  N/A (ByteCnt)                      0
    ---------------------------------------------------------------

IPV4 ACL Accounting Information
perPort[3/21] => Inbound ACL: 10
    0: permit host 10.10.10.1
     Hit Count:   (1Min)    N/A   (5Sec)                      N/A
                  (PktCnt)  N/A (ByteCnt)                        0
    ---------------------------------------------------------------
65535: Implicit Rule deny any any
     Hit Count:   (1Min)     N/A   (5Sec)                    N/A
                  (PktCnt)   N/A (ByteCnt)                 27452732
    ---------------------------------------------------------------

IPV6 ACL Accounting Information
perPort[3/21] => Inbound ACL: v6
    0:  permit ipv6 any any
     Hit Count:   (1Min)   N/A   (5Sec)                      N/A
                  (PktCnt) N/A (ByteCnt)                  1590514520
    ---------------------------------------------------------------
    1:  permit ipv6 1000::/64 2000::/64
     Hit Count:   (1Min)   N/A   (5Sec)                      N/A
                  (PktCnt)  N/A (ByteCnt)                      0
    ---------------------------------------------------------------
65533: Implicit ND_NA Rule: permit any any
     Hit Count:   (1Min)  N/A   (5Sec)                       N/A
                  (PktCnt)  N/A (ByteCnt)                      0
    ---------------------------------------------------------------
65534: Implicit ND_NS Rule: permit any any
     Hit Count:   (1Min)   N/A   (5Sec)                      N/A
                  (PktCnt) N/A (ByteCnt)                      0
```

```
    ------------------------------------------------------------------
65535: Implicit Rule: deny any any
     Hit Count:    (1Min)   N/A   (5Sec)                      N/A
                   (PktCnt) N/A (ByteCnt)                      0
    ------------------------------------------------------------------
```

The following output shows an Ethernet interface that has a MAC filter applied and ACL accounting enabled.

```
device# show access-list accounting ethernet 3/1/2 in

MAC Filters Accounting Information
    0: DA ANY SA 0000.0000.0001 - MASK FFFF.FFFF.FFFF
       action to take : DENY
     Hit Count:    (1Min)                      0    (5Sec)                  0
                   (PktCnt)                    0  (ByteCnt)                 0
    ------------------------------------------------------------------
65535: Implicit Rule deny any any
     Hit Count:    (1Min)            5028   (5Sec)                2129
                   (PktCnt)          5028 (ByteCnt)             643584
    ------------------------------------------------------------------
```

History

Release version	Command history
08.0.10	This command was introduced.

show acl-on-arp

Displays the list of ACLs that are configured to filter ARP requests.

Syntax

show acl-on-arp [**ethernet** *stack/slot/port* [**to** *stack/slot/port* | [**ethernet** *stack/slot/port* **to** *stack/slot/port* | **ethernet** *stack/slot/port*] ...] | **loopback** *num* | **tunnel** *num* | **ve** *num*]

Parameters

ethernet *stack/slot/port*

Displays the list of ACLs that are configured to filter ARP requests on a specific Ethernet interface.

to *stack/slot/port*

Displays the list of ACLs that are configured to filter ARP requests on a range of Ethernet interfaces.

loopback *num*

Displays the list of ACLs that are configured to filter ARP requests on a specific loopback interface.

tunnel *num*

Displays the list of ACLs that are configured to filter ARP requests on a specific tunnel interface.

ve *num*

Displays the list of ACLs that are configured to filter ARP requests on a specific VE interface.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Access list configuration mode

Usage Guidelines

The Filter Count column shows how many ARP packets have been dropped on the interface since the last time the count was cleared.

Examples

The following example displays a sample output of the **show acl-on-arp** command.

```
device(config)# show acl-on-arp
Port    ACL ID        Filter Count
2        103          10
3        102            23
4        101            12
```

show arp

Displays the ARP table.

Syntax

show arp

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

Use this command to view the total number of ARP entries and the maximum capacity for the ARP table along with the details of the ARP entries.

Command Output

The **show arp** command displays the following information:

Output field	Description
Total number of ARP entries	The total number of ARP entries in the table.
Maximum capacity	The maximum capacity of the ARP table.

Examples

The following example displays the ARP table.

```
device# show arp
Total number of ARP entries: 2, maximum capacity: 6000
No IP Address     MAC Address       Type    Age  Port    Status
1  10.43.1.1      0000.00a0.4000  Dynamic  0    mgmt1   Valid
2  10.43.1.78     0000.0060.6ab1  Dynamic  2    mgmt1   Valid
```

show auth-mac-addresses

Displays information about the MAC authentication configuration details.

Syntax

show auth-mac-addresses [*mac-address* | **authorized-mac**] [*ip-addr*]

show auth-mac-addresses [**detailed**] [**ethernet** *slot/port* [[**to** *slot/port*] [**ethernet** *slot/port*]...]]

show auth-mac-addresses [**configuration** | **unauthorized-mac**]

Parameters

mac-address
Displays MAC authentication information for a specific MAC address.

authorized-mac
Displays MAC addresses that are successfully authenticated.

ip-addr
Displays MAC authentication information with the IP address and ACL for the MAC address.

detailed
Displays detailed MAC authentication information.

ethernet *slot/port*
Displays the details of the port.

configuration
Displays MAC authentication configuration details.

unauthorized-mac
Displays MAC addresses for which authentication was not successful.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show auth-mac-addresses** commands displays the following information:

Output field	Description
Port	The port number where the MAC authentication feature is enabled.
Vlan	The VLAN to which the port has been assigned.
Accepted MACs	The number of MAC addresses that have been successfully authenticated.

Output field	Description
Rejected MACs	The number of MAC addresses for which authentication has failed.
Attempted-MACs	The rate at which authentication attempts are made for MAC addresses.
MAC/IP Address	The MAC address for which information is displayed. If the packet for which MAC authentication was performed also contained an IP address, then the IP address is displayed as well.
Port	The port on which the MAC address was learned.
Vlan	The VLAN to which the MAC address was assigned.
Authenticated	Whether the MAC address was authenticated.
Time	The time at which the MAC address was authenticated. If the clock is set on the Brocade device, then the actual date and time are displayed. If the clock has not been set, then the time is displayed relative to when the device was last restarted.
Age	The age of the MAC address entry in the authenticated MAC address list.
CAM Index	If the MAC address is blocked, this is the index entry for the Layer 2 CAM entry created for this MAC address. If the MAC address is not blocked, either through successful authentication or through being placed in the restricted VLAN, then "N/A" is displayed. If the hardware aging period has expired, then "ffff" is displayed for the MAC address during the software aging period.
MAC Address	The MAC addresses learned on the port. If the packet for which MAC authentication was performed also contained an IP address, the IP address is also displayed.
Dot1x	Indicates if 802.1X authentication is enabled or disabled for the MAC address.
Port	The port to which this information applies.
Dynamic-Vlan Assignment	Whether RADIUS dynamic VLAN assignment has been enabled for the port.
RADIUS failure action	What happens to traffic from a MAC address for which RADIUS authentication has failed: either the traffic is blocked or the MAC address is assigned to a restricted VLAN.
Failure restrict use dot1x	Indicates 802.1x traffic that failed MAC authentication, but succeeded 802.1x authentication to gain access to the network.
Override-restrict-vlan	Whether a port can be dynamically assigned to a VLAN specified by a RADIUS server, if the port had been previously placed in the restricted VLAN because a previous attempt at authenticating a MAC address on that port failed.
Port Default Vlan	The VLAN to which the port is assigned, and whether the port had been dynamically assigned to the VLAN by a RADIUS server.
Port VLAN State	Indicates the state of the port VLAN. The state can be one of the following: "Default", "RADIUS Assigned", or "Restricted".
802.1X override Dynamic PVID	Indicates if 802.1X can dynamically assign a Port VLAN ID (PVID).
override return to PVID	If a port PVID is assigned through MAC authentication, and 802.1X authentication subsequently specifies a different PVID, then the PVID specified through 802.1X authentication overrides the PVID specified through MAC authentication. This line indicates the PVID the port will use if 802.1X dynamically assigns a PVID.
Original PVID	The originally configured (not dynamically assigned) PVID for the port.
DOS attack protection	Whether Denial of Service attack protection has been enabled for MAC authentication, limiting the rate of authentication attempts sent to the RADIUS server.

Output field	Description
Accepted Mac Addresses	The number of MAC addresses that have been successfully authenticated.
Rejected Mac Addresses	The number of MAC addresses for which authentication has failed.
Authentication in progress	The number of MAC addresses for which authentication is pending. This is the number of MAC addresses for which an Access-Request message has been sent to the RADIUS server, and for which the RADIUS server has not yet sent an Access-Accept message.
Authentication attempts	The total number of authentication attempts made for MAC addresses on an interface, including pending authentication attempts.
RADIUS timeouts	The number of times the session between the Brocade device and the RADIUS server timed out.
RADIUS timeouts action	Action to be taken by the RADIUS server if it times out.
MAC Address on the PVID	Number of MAC addresses on the PVID.
MAC Address authorized on PVID	Number of authorized MAC addresses on the PVID.
Aging of MAC-sessions	Whether software aging of MAC addresses is enabled.
Port move-back vlan	Indicates the destination VLAN when a RADIUS-assigned VLAN is removed. By default, it would return the configured VLAN.
Max-Age of sw mac-sessions	The configured software aging period for MAC addresses.
hw age for denied mac	The hardware aging period for blocked MAC addresses. The MAC addresses are dropped in hardware once the aging period expires.
MAC Filter applied	Indicates whether a MAC address filter has been applied to this port to specify pre-authenticated MAC addresses.
Dynamic ACL applied	Indicates whether a dynamic ACL was applied to this port.
num Dynamic Tagged Vlan	The number of dynamically tagged VLANs on this port.
Dynamic Tagged Vlan list	The list of dynamically tagged VLANs on this port. In the following example, 1025 (1/1) indicates that there was one MAC session and one learned MAC address for VLAN 1025. Likewise, 4060 (1/0) indicates that there was one MAC session and no learned MAC addresses for VLAN 4060.
MAC Address	The MAC addresses learned on the port. If the packet for which MAC authentication was performed also contained an IP address, then the IP address is displayed as well.
RADIUS Server	The IP address of the RADIUS server used for authenticating the MAC addresses.
Authenticated	Whether the MAC address has been authenticated by the RADIUS server.
Time	The time at which the MAC address was authenticated. If the clock is set on the Brocade device, then the actual date and time are displayed. If the clock has not been set, then the time is displayed relative to when the device was last restarted.
Age	The age of the MAC address entry in the authenticated MAC address list.
Dot1x	Indicates if 802.1X authentication is enabled or disabled for the MAC address.
Feature enabled	Whether MAC authentication is enabled on the Brocade device.
Number of Ports enabled	The number of ports on which the MAC authentication feature is enabled.
Port	Information for each MAC authentication-enabled port.

Output field	Description
Fail-Action	What happens to traffic from a MAC address for which RADIUS authentication has failed either block the traffic or assign the MAC address to a restricted VLAN.
Fail-vlan	The restricted VLAN to which non-authenticated MAC addresses are assigned, if the Fail-Action is to assign the MAC address to a restricted VLAN.
Dyn-vlan	Whether RADIUS dynamic VLAN assignment is enabled for the port.
MAC-filter	Whether a MAC address filter has been applied to specify pre-authenticated MAC addresses.

Examples

The following example displays information about authenticated MAC addresses on the ports where MAC authentication is enabled.

```
device# show auth-mac-addresses
-------------------------------------------------------------------
Port          Vlan      Accepted MACs    Rejected MACs   Attempted-MACs
-------------------------------------------------------------------
1/18          100       1                100             0
1/20          40        0                0               0
1/22          100       0                0               0
4/5           30        0                0               0
```

The following example displays authentication information for a specific MAC address or port.

```
device# show auth-mac-addresses 0000.000f.eaa1
-------------------------------------------------------------------------------------
MAC / IP Address             Port  Vlan Authenticated   Time         Age   CAM Index
-------------------------------------------------------------------------------------
0000.000f.aaa1: 10.25.25.25  1/18  100  Yes             00d01h10m06s  0     N/A
```

The following example displays the MAC addresses that are successfully authenticated.

```
device# show auth-mac-addresses authorized-mac
-------------------------------------------------------------------------------
MAC Address               Port      Vlan    Authenticated  Time          Age   dot1x
-------------------------------------------------------------------------------
0000.0074.3181            15/23     101     Yes            00d01h03m17s  Ena   Ena
0000.0000.0001            18/1      87      Yes            00d01h03m17s  Ena   Ena
0000.0000.012d            18/1      87      Yes            00d01h03m17s  Ena   Ena
0000.0000.0065            18/1      87      Yes            00d01h03m17s  Ena   Ena
0000.0000.0191            18/1      87      Yes            00d01h03m17s  Ena   Ena
0000.0000.01f5            18/1      87      Yes            00d01h03m17s  Ena   Ena
```

The following example displays MAC authentication information for a port.

```
device# show auth-mac-addresses ethernet 18/1
-------------------------------------------------------------------------
MAC Address          Port     Vlan   Authenticated  Time          Age     Dot1x
-------------------------------------------------------------------------
0000.0000.0001       18/1     87     Yes            00d01h03m17s  Ena     Ena
0000.0000.012d       18/1     87     Yes            00d01h03m17s  Ena     Ena
0000.0000.0321       18/1     87     No             00d01h03m17s  H52     Ena
0000.0000.0259       18/1     87     No             00d01h03m17s  H52     Ena
0000.0000.0065       18/1     87     Yes            00d01h03m17s  Ena     Ena
0000.0000.0385       18/1     87     No             00d01h03m17s  H52     Ena
0000.0000.0191       18/1     87     Yes            00d01h03m17s  Ena     Ena
0000.0000.02bd       18/1     87     No             00d01h03m17s  H52     Ena
0000.0000.00c9       18/1     87     No             00d01h03m17s  H52     Ena
```

The following example displays MAC authentication settings and authenticated MAC addresses for a port where the MAC authentication is enabled.

```
device# show auth-mac-addresses detailed ethernet 15/23
Port                              : 15/23
Dynamic-Vlan Assignment           : Enabled
RADIUS failure action             : Block Traffic
Failure restrict use dot1x        : No
Override-restrict-vlan            : Yes
Port Default VLAN                 : 101 ( RADIUS assigned: No) (101)
Port Vlan State                   : DEFAULT
802.1x override Dynamic PVID      : YES
override return to PVID           : 101
Original PVID                     : 101
DOS attack protection             : Disabled
Accepted Mac Addresses            : 1
Rejected Mac Addresses            : 0
Authentication in progress        : 0
Authentication attempts           : 0
RADIUS timeouts                   : 0
RADIUS timeouts action            : Success
MAC Address on PVID               : 1
MAC Address authorized on PVID    : 1
Aging of MAC-sessions             : Enabled
Port move-back vlan               : Port-configured-vlan
Max-Age of sw mac session         : 120 seconds
hw age for denied mac             : 70 seconds
MAC Filter applied                : No
Dynamic ACL applied               : No
num Dynamic Tagged Vlan           : 2
Dynamic Tagged Vlan list          : 1025 (1/1) 4060 (1/0)
-------------------------------------------------------------------------------
MAC Address          RADIUS Server     Authenticated    Time          Age  Dot1x
-------------------------------------------------------------------------------
0000.0074.3181       10.12.12.5        Yes              00d01h03m17s  Ena  Ena
```

The following example displays the MAC addresses for which authentication was not successful.

```
device# show auth-mac-addresses unauthorized-mac
-------------------------------------------------------------------------------
MAC Address             Port     Vlan      Authenticated     Time          Age    dot1x
-------------------------------------------------------------------------------
0000.0000.0321          18/1     87        No                00d01h03m17s  H44    Ena
0000.0000.0259          18/1     87        No                00d01h03m17s  H44    Ena
0000.0000.0385          18/1     87        No                00d01h03m17s  H44    Ena
0000.0000.02bd          18/1     87        No                00d01h03m17s  H44    Ena
0000.0000.00c9          18/1     87        No                00d01h03m17s  H44    Ena
```

The following example displays information about the MAC authentication configuration.

```
device# show auth-mac-addresses configuration
Feature enabled : Yes
Number of Ports enabled : 4
-------------------------------------------------------------------------
Port       Fail-Action       Fail-vlan   Dyn-vlan   MAC-filter
-------------------------------------------------------------------------
1/18       Block Traffic     1           No         No
1/20       Block Traffic     1           No         No
1/22       Block Traffic     1           No         Yes
4/5        Block Traffic     1           No         No
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

show boot-preference

Displays the boot sequence in the startup configuration and running configuration files.

Syntax

show boot-preference

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

All configuration modes

Usage Guidelines

The boot sequence displayed is also identified as either user-configured or the default.

Examples

The following example shows the default boot sequence preference.

```
device# show boot-preference

Boot system preference (Configured):
            Use Default
Boot system preference(Default):
            Boot system flash primary
            Boot system flash secondary
```

The following example shows a user-configured boot sequence preference.

```
device# show boot-preference

Boot system preference(Configured):
            Boot system flash primary
Boot system preference(Default):
            Boot system flash primary
            Boot system flash secondary
```

show breakout

Displays information on 10 Gbps sub-ports broken out from 40 Gbps ports on certain FastIron devices.

Syntax

show breakout

Modes

Privileged EXEC mode.

Usage Guidelines

The **show breakout** command is available only on ICX 7750 devices.

Command Output

The **show breakout** command displays the following information:

Output field	Description
Port	Specifies the port for which breakout information is displayed to the right.
Module Exist	Indicates whether the module on which the specified port resides is present in the unit.
Module Conf	Indicates whether the module on which the specified port resides is configured.
Breakout-config	Indicates whether breakout is configured on the specified port.
Breakout-oper	Indicates whether sub-ports on the specified breakout port are operational.

Examples

The following example shows that port 1/2/1 has been configured for breakout into four 10 Gbps sub-ports and is operational (has active sub-ports). Ports 1/2/2 and 1/2/4 are configured for breakout, pending reload.

```
Device# show breakout
Unit-Id: 1
Port         Module Exist  Module Conf    Breakout-config   Breakout-oper
1/2/1        yes           no             yes               yes
1/2/2        yes           no             yes               no
1/2/3        yes           no             no                no
1/2/4        yes           no             yes               no
1/2/5        yes           no             no                no
1/2/6        yes           no             no                no
1/3/1        yes           no             no                no
1/3/2        yes           no             no                no
1/3/3        yes           no             no                no
1/3/4        yes           no             no                no
1/3/5        yes           no             no                no
1/3/6        yes           no             no                no
```

History

Release version	Command history
FastIron Release 08.0.30	This command was introduced.

show cable-diagnostics tdr

Displays the results of Virtual Cable Test (VCT) TDR cable diagnostic testing.

Syntax

show cable-diagnostics tdr *stackid/slot/ port*

Parameters

stackid/slot/port Identifies the specific interface (port), by device, slot, and port number in the format shown.

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

Most Brocade devices support VCT technology. VCT technology enables the diagnosis of a conductor (wire or cable) by sending a pulsed signal into the conductor, then examining the reflection of that pulse. This method of cable analysis is referred to as Time Domain Reflectometry (TDR). By examining the reflection, the Brocade device can detect and report cable statistics such as local and remote link pair, cable length, and link status.

THis command is supported only on the Brocade ICX 6610, ICX 6430, ICX 6430-C, ICX 6450, and ICX6450-C.

Examples

The following example displays TDR test results for port 1, slot 2 on device 3 in the stack. The results indicate that the port is down or the cable is not connected.

```
device>show cable-diagnostics tdr 3/2/1

Port      Speed Local pair Pair Length Remote pair Pair status
--------- ----- ---------- ----------- ----------- -----------
01        UNKWN Pair A     >=3 M                   Open
                Pair B     >=3 M                   Open
                Pair C     >=3 M                   Open
                Pair D     >=3 M                   Open
```

The following example displays I the TDR test results for the same port show details for an active port.

```
device>show cable-diagnostics tdr 3/2/1

Port      Speed Local pair Pair Length Remote pair Pair status
--------- ----- ---------- ----------- ----------- -----------
01        1000M Pair A     50M         Pair B      Terminated
                Pair B     50M         Pair A      Terminated
                Pair C     50M         Pair D      Terminated
                Pair D     50M         Pair C      Terminated
```

History

Release version	Command history
08.0.20	This command was introduced.

show captive-portal

Displays the details of the Captive Portal profile configured on the device.

Syntax

show captive-portal *profile-name*

Parameters

profile-name

Specifies a specific Captive Portal profile configured on the device.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Web Authentication configuration mode

Command Output

The **show captive-portal** command displays the following information:

Output field	Description
cp-name	The local account username.
virtual-ip	The IP address of the Aruba ClearPass server.
virtual-port	The port number to facilitate HTTP services for the client. The port can be secure HTTPS port 443 or unsecure HTTP port 80.
login-page	The login-page hosted on the external web server.

Examples

The following example displays the details for the cp-brocade Captive Portal profile.

```
device(config)# show captive-portal cp-brocade
Configured Captive Portal Profile Details :
  cp-name               :cp-brocade
  virtual-ip            :10.21.240.42
  virtual-port          :80
  login-page            :/guest/brocadeguestlogin.php
```

History

Release version	Command history
8.0.40	This command was introduced.

Release version	Command history
8.0.30j	This command was added to FastIron 8.0.30j

show chassis

Displays chassis information for each stack unit.

Syntax

show chassis

Command Output

The **show chassis** command output displays the following information.

Output field	Description
Power supply #	The presence, status, output type, model number, serial number, and firmware version number of the power supply units, if present.
Power supply # Fan Air Flow Direction	The air flow direction of the power supply unit.
Fan #	The presence, status, speed mode, and air flow direction of the fan. The fan controlled temperature and temperature thresholds.
MAC # Temperature Readings	The current temperature reading of the MAC device.
CPU Temperature Readings	The current temperature reading of the CPU.
sensor # Temperature Readings	The current temperature reading of the sensor.
Boot Prom MAC	The MAC address of the boot prom.
Management MAC	The management MAC address, for the active controller only.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show chassis** command executed on an ICX 6610 device.

```
Brocade# show chassis
The stack unit 1 chassis info:

Power supply 1 not present
Power supply 2 (AC - Regular) present, status ok
        Model Number:   23-0000143-01
        Serial Number:  F00E
        Firmware Ver:    0
Power supply 2 Fan Air Flow Direction:  Back to Front

Fan 1 ok, speed (auto): [[1]]<->2
Fan 2 not present

Fan controlled temperature: 64.0 deg-C

Fan speed switching temperature thresholds:
               Speed 1: NM<----->82       deg-C
               Speed 2:       77<-----> 86 deg-C (shutdown)

Fan 1 Air Flow Direction:Back to Front
MAC 1 Temperature Readings:
        Current temperature : 47.5 deg-C
CPU Temperature Readings:
        Current temperature : 64.0 deg-C
sensor A Temperature Readings:
        Current temperature : 45.5 deg-C
sensor B Temperature Readings:
        Current temperature : 48.0 deg-C
sensor C Temperature Readings:
        Current temperature : 35.5 deg-C
stacking card Temperature Readings:
        Current temperature : 60.5 deg-C
        Warning level.......: 70.0 deg-C
        Shutdown level......: 86.0 deg-C
Boot Prom MAC : 0000.0034.289c
```

NOTE

The output of the **show chassis** command is different for ICX 6610 devices and FastIron SX devices.

History

Release	Command History
08.0.00a	This command was enhanced to display model number, serial number, and firmware version number for power supply units.

show cluster ccp

Displays information about Cluster Communication Protocol (CCP) of the cluster.

Syntax

show cluster { *cluster-name* | *cluster-id* } **ccp** [**buffered-messages** | **peer** [*ip-address*] [**detail**] | **client** *client-id*]

Parameters

cluster-name
: Specifies the name of the cluster.

cluster-id
: Specifies the cluster ID.

buffered-messages
: Displays the number of CCP messages.

peer *ip-address*
: Displays the information for the cluster peer identified by the IP address.

detail
: Displays the detailed peer information.

client *client-id*
: Displays the information for the client identified by the client ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

Usage Guidelines

The **show cluster ccp** command is available only on FSX devices.

Examples

The following example displays sample output of the **show cluster ccp** command.

```
device# show cluster 1 ccp peer
...
PEER IP ADDRESS       STATE             UP TIME
---------------       -------------     --------------
 10.1.1.1             OPERATIONAL       0 days: 2 hr:25 min:16 sec
```

The following example displays sample output of the **show cluster ccp peer detail** command:

```
device# show cluster 1 ccp peer detail
**************Peer Session Details*********************
IP address of the peer                          10.1.1.1
Rbridge ID of the peer                          100
Session state of the peer                       OPERATIONAL
Next message ID to be send                      287
Keep Alive interval in seconds                  30
Hold Time Out in seconds                        90
Fast Failover is enable for the session
UP Time                                          0 days: 2 hr:22 min:58 sec
Number of  tcp packet allocations failed           0
Message    Init          Keepalive     Notify        Application   Badmessages
Send       3             2421          2             53            0
Receive    3             2415          0             37            0
TCP connection is up
TCP connection is initiated by                  10.1.1.2
TCP connection tcbHandle not pending
TCP connection  packets not received
**************TCP Connection Details********************
    TCP Connection state: ESTABLISHED      Maximum segment size: 1436
       Local host:  10.1.1.2, Local  Port: 12203
       Remote host: 10.1.1.1, Remote Port: 4175
       ISentSeq: 1867652277  SendNext: 1867660731  TotUnAck:          0
       TotSent:        8454  ReTrans:           9  UnAckSeq: 1867660731
       IRcvSeq:  3439073167  RcvNext:  3439078415  SendWnd:       16384
       TotalRcv:       5248  DupliRcv:         16  RcvWnd:        16384
       SendQue:           0  RcvQue:            0  CngstWnd:       1452
```

show cluster client

Displays the cluster additional state machine information.

Syntax

show cluster [*cluster-name* | *cluster-id*] **client** [*client-name* | *client-rbridgeid*]

Parameters

cluster-name
: Specifies the configured cluster name.

cluster-id
: Specifies the configured cluster ID.

client-name
: Specifies the cluster client name.

client-rbridgeid
: Specifies the client RBridge ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

Usage Guidelines

The **show cluster client** command is available only on FSX devices .

You can specify an individual cluster and client.

Examples

The following example displays sample output of the **show cluster client** command.

```
device# show cluster 1 client
Cluster 1 1
==================
Rbridge Id: 101, Session Vlan: 3999, Keep-Alive Vlan: 4001
Cluster State: Deploy
Client Isolation Mode: Loose
Configured Member Vlan Range: 100 to 105
Active Member Vlan Range: 100 to 105
MCT Peer's Reachability status using Keep-Alive Vlan: Peer Reachable
Client Info:
------------
Client: c1, rbridge-id: 300, Deployed
Client Port: 3/11
State: Up
Number of times Local CCEP down: 0
Number of times Remote CCEP down: 0
Number of times Remote Client undeployed: 0
Total CCRR packets sent: 4
Total CCRR packets received: 3
```

show cluster config

Displays the peer device and client states of the cluster.

Syntax

show cluster [*cluster-name* | *cluster-id*] **config**

Parameters

cluster-name

Specifies the cluster name.

cluster-id

Specifies the cluster ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

Usage Guidelines

The **show cluster config** command is available only on FSX devices.

Use the **show cluster** command without any options to display the general cluster information.

Examples

The following example displays sample output of the **show cluster config** command.

```
device# show cluster SXR122 config
cluster SXR122 100
rbridge-id 100
session-vlan 1
keep-alive-vlan 3
icl SXR122-MCT ethernet 1/1/1
peer 172.17.0.2 rbridge-id 101 icl SXR122-MCT
deploy
client KL134
rbridge-id 14
client-interface ethernet 1/1/23
deploy
client AGG131
rbridge-id 10
client-interface ethernet 1/2/2
deploy
client FOX135
rbridge-id 15
client-interface ethernet 1/2/5
deploy
```

show configuration

Displays the configuration data in startup configuration file.

Syntax

show configuration

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

All configuration modes

Examples

The following example is a sample output of the **show configuration** command.

```
device# show configuration
!
Startup-config data location is flash memory
!
Startup configuration:
!
ver 08.0.20
!
stack unit 1
  module 1 icx7450-24-port-management-module
  module 2 icx7400-xgf-4port-40g-module
  module 3 icx7400-qsfp-1port-40g-module
  module 4 icx7400-qsfp-1port-40g-module
!
!
!
!
!
!
!
boot sys fl sec
ip address 10.25.224.197 255.255.255.0 dynamic
ip dns domain-list englab.brocade.com
ip dns server-address 10.31.2.10
ip default-gateway 10.25.224.1
!
!
!
!
!
!
!
!
!
!
end
```

show cpu

Displays the CPU histogram for the device, and optionally, the CPU utilization for each task running on the device.

Syntax

show cpu [**tasks**]

Parameters

tasks

Displays the CPU utilization for each task running on the device.

Modes

Global configuration mode

User EXEC

Usage Guidelines

Examples

The following example displays the CPU histogram for the device.

```
device# show cpu
1 percent busy, from 4267 sec ago
1   sec avg:  1 percent busy
5   sec avg:  1 percent busy
60  sec avg:  1 percent busy
300 sec avg:  1 percent busy
```

The following example displays the CPU utilization for each task on the device.

```
device# show cpu tasks
... Usage average for all tasks in the last 1 second ...
=========================================================
Name                                    %

SigHdlrTsk                              0
OsTsk                                   0
TimerTsk                                0
FlashTsk                                0
MainTsk                                 0
MportPollTsk                            0
IntrTsk                                 0
keygen                                  0
itc                                     0
bcmDPC                                  0
bcmINTR                                 3
socdmadesc.0                            0
bcmCNTR.0                               3
bcmTX                                   0
bcmXGS3AsyncTX                          0
bcmRX                                   0
bcmL2MOD.0                              0
scp                                     0
appl                                    86
snms                                    0
rtm                                     0
rtm6                                    0
rip                                     0
bgp                                     0
bgp_io                                  0
ospf                                    0
ospf_r_calc                             0
mcast_fwd                               0
mcast                                   0
msdp                                    0
ripng                                   0
ospf6                                   0
ospf6_rt                                0
mcast6                                  0
ipsec                                   0
dhcp6                                   0
snmp                                    0
rmon                                    0
web                                     0
acl                                     0
ntp                                     0
console                                 0
ospf_msg_task                           0
auxTsk                                  0
```

History

Release version	Command history
08.0.30	This command was introduced.

show cpu histogram

Displays the CPU usage histogram for the device, and optionally, clears the hold time and wait time.

Syntax

show cpu histogram [**clear** | **holdtime** | **waittime**]

Parameters

clear

Displays the CPU usage histogram and clears the hold time and wait time.

holdtime

Displays the CPU hold time usage histogram.

waittime

Displays the CPU wait time usage histogram.

Modes

Global configuration mode

User EXEC

Usage Guidelines

Command Output

The **show cpu histogram** command displays the following information:

Output field	Description
No. of buckets	The CPU usage histogram is presented in the form of buckets. Usage is divided into different intervals called buckets.
Bucket granularity	The time interval at which the CPU usage information is collected for each bucket.
Last clear	The datestamp when the task was cleared last.

Examples

The following command displays the CPU hold time usage histogram.

```
device# show cpu histogram holdtime

CPU Histogram Info
------------------
No. of Buckets     : 11
Bucket Granularity : 50 msec
No. of Tasks       : 14
Last clear         : Jan  1 18:11:39.414

-------------------------------------------------------------------------------------------------------
 Task                |   Bkt |  Bkt      | Total      | Last         | Max          |     Max Hold at    |
 Name                |   Num |  Time(ms)| Count      | HoldTime(ms)| HoldTime(ms)|
                     |
-------------------------------------------------------------------------------------------------------
appl                       1     000-050  758226345         9.521        46.543
Jan  1 18:50:16.857
appl                       2     050-100          4        50.967        52.324
Jan  1 18:46:00.638
rtm                        1     000-050      44197         0.008         0.283
Jan  1 18:33:37.651
rtm6                       1     000-050      44197         0.005         0.415
Jan  1 18:18:31.476
ospf                       1     000-050      44197         0.004         1.177
Jan  1 19:02:29.746
openflow_opm               1     000-050       9118         0.007         0.239
Jan  1 18:15:01.952
mcast                      1     000-050      90565         0.004         0.143
Jan  1 18:29:04.325
msdp                       1     000-050       4425         0.007         0.201
Jan  1 19:15:34.419
ospf6                      1     000-050      44197         0.007         0.257
Jan  1 18:44:58.033
mcast6                     1     000-050      90565         0.004         0.181
Jan  1 18:36:38.346
rmon                       1     000-050       4425         0.028         5.787
Jan  1 19:24:47.464
web                        1     000-050      88335         0.010         0.368
Jan  1 18:29:48.222
acl                        1     000-050       2360         0.015         0.177
Jan  1 18:22:40.049
ntp                        1     000-050       4425         0.007         0.011
Jan  1 18:11:40.713
console                    1     000-050      88337         0.008        35.227
Jan  1 18:11:39.498
-------------------------------------------------------------------------------
--------------------
```

The following example displays the CPU wait time usage histogram.

```
device# show cpu histogram waittime
CPU Histogram Info
------------------
No. of Buckets     : 11
Bucket Granularity : 50 msec
No. of Tasks       : 14
Last clear         : Jan  1 18:11:39.414

-------------------------------------------------------------------------------------------------------
 Task                |   Bkt |  Bkt     | Total     | Last         | Max          |     Max Wait at   |
 Name                |   Num |  Time(ms)| Count     | WaitTime(ms)| WaitTime(ms)|
                     |
-------------------------------------------------------------------------------------------------------
rtm                        1     000-050      44876         0.008         0.283
Jan  1 18:50:16.857
rtm6                       1     000-050      44876         0.005         0.415
Jan  1 18:50:16.857
ospf                       1     000-050      44876         0.065         1.177
Jan  1 18:50:16.857
openflow_opm               1     000-050       9258         0.006         0.239
Jan  1 19:07:56.599
mcast                      1     000-050      91957         0.005         0.143
Jan  1 18:50:16.857
msdp                       1     000-050       4493         0.008         0.201
Jan  1 18:28:40.956
ospf6                      1     000-050      44876         0.007         0.257
Jan  1 18:50:16.857
mcast6                     1     000-050      91957         0.004         0.181
Jan  1 18:50:16.857
rmon                       1     000-050       4493         0.030         5.787
Jan  1 18:28:40.956
web                        1     000-050      89691         0.009         0.368
Jan  1 18:50:16.857
acl                        1     000-050       2397         0.018         0.177
Jan  1 18:33:17.172
ntp                        1     000-050       4493         0.007         0.011
Jan  1 18:28:40.956
console                    1     000-050      89693         0.010        35.227
Jan  1 18:50:16.857
-------------------------------------------------------------------------------
```

The following example clears the CPU usage histogram information.

```
device# show cpu histogram clear

CPU Histogram Info
------------------
No. of Buckets     : 11
Bucket Granularity : 50 msec
No. of Tasks       : 14
Last clear         : Jan  1 18:11:39.414

-------------------------------------------------------------------------------------------------------
 Task                |   Bkt |  Bkt     | Total     | Last         | Max          |     Max Hold at    |
 Name                |   Num |  Time(ms)| Count     | HoldTime(ms)| HoldTime(ms)|
                     |
-------------------------------------------------------------------------------------------------------
appl                       1     000-050   793262215        0.003        46.543
Jan  1 18:50:16.857
appl                       2     050-100           4       50.967        52.324
Jan  1 18:46:00.638
rtm                        1     000-050       46242         0.009         0.283
Jan  1 18:33:37.651
rtm6                       1     000-050       46242         0.005         0.415
Jan  1 18:18:31.476
ospf                       1     000-050       46242         0.006         1.177
Jan  1 19:02:29.746
openflow_opm               1     000-050        9540         0.007         0.239
Jan  1 18:15:01.952
mcast                      1     000-050       94771         0.003         0.143
Jan  1 18:29:04.325
msdp                       1     000-050        4629         0.008         0.201
Jan  1 19:15:34.419
ospf6                      1     000-050       46242         0.006         0.257
Jan  1 18:44:58.033
mcast6                     1     000-050       94771         0.003         0.181
Jan  1 18:36:38.346
rmon                       1     000-050        4629         0.137         5.787
Jan  1 19:24:47.464
web                        1     000-050       92421         0.007         0.368
Jan  1 18:29:48.222
acl                        1     000-050        2470         0.006         0.177
Jan  1 18:22:40.049
ntp                        1     000-050        4629         0.006         0.011
Jan  1 18:11:40.713
console                    1     000-050       92423         0.008        35.227
Jan  1 18:11:39.498
-------------------------------------------------------------------------------------------------------

CPU Histogram Info
------------------
No. of Buckets     : 11
Bucket Granularity : 50 msec
No. of Tasks       : 14
Last clear         : Jan  1 18:11:39.414

-------------------------------------------------------------------------------------------------------
 Task                |   Bkt |  Bkt     | Total     | Last         | Max          |     Max Wait at    |
 Name                |   Num |  Time(ms)| Count     | WaitTime(ms)| WaitTime(ms)|
                     |
-------------------------------------------------------------------------------------------------------
rtm                        1     000-050       46242         0.009         0.283
Jan  1 18:50:16.857
rtm6                       1     000-050       46242         0.005         0.415
Jan  1 18:50:16.857
ospf                       1     000-050       46242         0.006         1.177
Jan  1 18:50:16.857
openflow_opm               1     000-050        9540         0.007         0.239
Jan  1 19:07:56.599
mcast                      1     000-050       94771         0.003         0.143
Jan  1 18:50:16.857
msdp                       1     000-050        4629         0.008         0.201
```

```
Jan  1 18:28:40.956
ospf6                    1     000-050      46242         0.006         0.257
Jan  1 18:50:16.857
mcast6                   1     000-050      94771         0.003         0.181
Jan  1 18:50:16.857
rmon                     1     000-050       4629         0.137         5.787
Jan  1 18:28:40.956
web                      1     000-050      92421         0.007         0.368
Jan  1 18:50:16.857
acl                      1     000-050       2470         0.006         0.177
Jan  1 19:28:22.095
ntp                      1     000-050       4629         0.006         0.011
Jan  1 18:28:40.956
console                  1     000-050      92423         0.008        35.227
Jan  1 18:50:16.857
-------------------------------------------------------------------------------------------------
CPU Histogram data cleared
```

History

Release version	Command history
08.0.30	This command was introduced.

show default values

Displays default, maximum, current, and configured values for system maximum parameters.

Syntax

show default values

Modes

Privileged EXEC mode

Examples

This example does not show complete output; it shows only PIM hardware mcache values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
pim-hw-mcache         1024       6144       1500       1500
```

This example does not show complete output; it shows only PIM6 hardware mcache values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
pim6-hw-mcache        512        1024       1024       1024
```

This example does not show complete output; it shows only MLD mcache values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
mld-snoop-mcache      512        8192       512        512
```

This example does not show complete output; it shows only IGMP group values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
igmp-snoop-group-add  4096       8192       5000       5000
```

This example does not show complete output; it shows only MLD group values.

```
Device(config)#show default values
System Parameters     Default    Maximum    Current    Configured
MLD-snoop-group-addr  4096       8192       5000       5000
```

show dir

Displays a list of the files stored in flash memory.

Syntax

show dir

Modes

Monitor mode

All configuration modes

Usage Guidelines

For devices other than FCX and ICX, enter the **dir** command at the monitor mode. To enter monitor mode from any level of the CLI, press the Shift and Control+Y keys simultaneously then press the M key. To exit monitor mode and return to the CLI, press Control+Z .

For FCX devices, enter the **show dir** command at any level of the CLI, or enter the **dir** command at the monitor mode.

For ICX devices, enter the **show dir** command at the device configuration prompt.

Examples

The following example is a sample output of the **show dir** command.

```
device# show dir

0             [ffff]        bootrom
3802772 [0000]        primary
4867691    [0000]        secondary
163        [dd8e]        stacking.boot
1773       [0d2d]     startup-config
1808       [acfa]        startup-config.backup
8674340    bytes 7 File(s)
```

show dlb-internal-trunk-hash

Displays the dynamic load balancing (DLB) hashing method for inter-packet-processor (inter-pp) links that connect master and slave units in ICX 7450-48 devices.

Syntax

show dlb-internal-trunk-hash

Modes

Global configuration mode

Examples

The following example displays the hashing method in effect for inter-pp links on an ICX 7450-48 device.

```
ICX7450-48P Router(config)#show dlb-internal-trunk-hash
Internal trunk mode: spray-mode
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x

Displays information about the 802.1X configuration.

Syntax

show dot1x

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

dot1x configuration mode

Command Output

The **show dot1x** command displays the following information:

Output field	Description
PAE Capability	The Port Access Entity (PAE) role for the Brocade device. This is always "Authenticator Only".
system-auth-control	Whether system authentication control is enabled on the device. The **dot1x-enable** command enables system authentication control on the device.
re-authentication	Whether periodic re-authentication is enabled on the device. When periodic re-authentication is enabled, the device automatically re-authenticates clients every 3,600 seconds by default.
global-filter-strict-security	Whether strict security mode is enabled or disabled globally.
quiet-period	When the Brocade device is unable to authenticate a client, the amount of time the Brocade device waits before trying again (default 60 seconds).
tx-period	When a client does not send back an EAP-response/identity frame, the amount of time the Brocade device waits before retransmitting the EAP-request/identity frame to a client (default 30 seconds).
supptimeout	When a client does not respond to an EAP-request frame, the amount of time before the Brocade device retransmits the frame.
servertimeout	When the Authentication Server does not respond to a message sent from the client, the amount of time before the Brocade device retransmits the message.
maxreq	The number of times the Brocade device retransmits an EAP-request/identity frame if it does not receive an EAP-response/identity frame from a client (default 2 times).
reAuthMax	The maximum number of re-authentication attempts.
re-authperiod	How often the device automatically re-authenticates clients when periodic re-authentication is enabled (default 3,600 seconds).
Protocol Version	The version of the 802.1X protocol in use on the device.

Examples

The following example displays information about the 802.1X configuration.

```
device# show dot1x
PAE Capability                    : Authenticator Only
system-auth-control               : Enable
re-authentication                 : Disable
global-filter-strict-security     : Enable
quiet-period                      : 60 Seconds
tx-period                         : 30 Seconds
supptimeout                       : 30 Seconds
servertimeout                     : 30 Seconds
maxreq                            : 2
reAuthMax                         : 2
re-authperiod                     : 3600 Seconds
Protocol Version                  : 1
```

show dot1x configuration

Displays detailed information about the 802.1X configuration.

Syntax

show dot1x configuration[**all** | **ethernet** *slot/port*]

Parameters

all

Displays information about the 802.1X configuration on all ports.

ethernet *slot/port*

Displays information about the 802.1X configuration on a specific port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

dot1x configuration mode

Command Output

The **show dot1x configuration** command displays the following information:

Output field	Description
PAE Capability	The Port Access Entity (PAE) role for the Brocade device. This is always "Authenticator Only".
system-auth-control	Whether system authentication control is enabled on the device. The **dot1x-enable** command enables system authentication control on the device.
Number of Ports enabled	The number of ports on which 802.1X authentication is enabled.
Re-authentication	Whether periodic re-authentication is enabled on the device. When periodic re-authentication is enabled, the device automatically re-authenticates clients every 3,600 seconds by default.
Authentication-fail-action	The configured authentication-failure action. This can be Restricted VLAN or Block Traffic.
Mac Session Aging	Whether aging for dot1x-MAC-sessions has been enabled or disabled for permitted or denied dot1x-MAC-sessions.
Mac Session max-age	The configured software aging time for dot1x-MAC-sessions.
Protocol Version	The version of the 802.1X protocol in use on the device.
quiet-period	When the Brocade device is unable to authenticate a client, the amount of time the Brocade device waits before trying again (default 60 seconds).
tx-period	When a client does not send back an EAP-response/identity frame, the amount of time the Brocade device waits before retransmitting the EAP-request/identity frame to a client (default 30 seconds).
supptimeout	When a client does not respond to an EAP-request frame, the amount of time before the Brocade device retransmits the frame.

Output field	Description
servertimeout	When the Authentication Server does not respond to a message sent from the client, the amount of time before the Brocade device retransmits the message.
maxreq	The number of times the Brocade device retransmits an EAP-request/identity frame if it does not receive an EAP-response/identity frame from a client (default 2 times).
reAuthmax	The maximum number of re-authentication attempts.
re-authperiod	How often the device automatically re-authenticates clients when periodic re-authentication is enabled (default 3,600 seconds).
global strict security	Whether strict security mode is enabled or disabled globally.

The **show dot1x configuration ethernet** *slot/port* command displays the following information:

Output field	Description
Port-Control	The configured port control type for the interface. This can be one of the following types: • force-authorized: The controlled port is placed unconditionally in the authorized state, allowing all traffic. This is the default state for ports on the Brocade device. • force-unauthorized: The controlled port is placed unconditionally in the unauthorized state. No authentication takes place for any connected 802.1X clients. • auto - The authentication status for each 802.1X client depends on the authentication status returned from the RADIUS server.
filter strict security	Whether strict security mode is enabled or disabled on the interface.
Action on RADIUS timeout	The action taken for the client MAC session on this port upon a RADIUS timeout.
Authentication-fail-action	The configured authentication-failure action. This can be Restricted VLAN or Block Traffic.
PVID State	The port default VLAN ID (PVID) and the state of the port PVID. The PVID state can be one of the following: • Normal - The port PVID is not set by a RADIUS server, nor is it the restricted VLAN. • RADIUS - The port PVID was dynamically assigned by a RADIUS server. • RESTRICTED - The port PVID is the restricted VLAN.
Original PVID	The originally configured (not dynamically assigned) PVID for the port.
Authorized PVID ref count	The number of authenticated MAC sessions on this port's current PVID (port default VLAN ID).
Restricted PVID ref count	The number of MAC sessions on the port that failed authentication and are now in the restricted VLAN (which should be the port's current PVID).
Radius assign PVID ref count	The number of times the port has changed PVIDs due to RADIUS VLAN assignment.
num mac sessions	The number of dot1x-MAC-sessions on the port.
num mac authorized	The number of authorized dot1x-MAC-sessions on the port.
num Dynamic Tagged Vlan	The number of dynamically tagged VLANs on the port.
Number of Auth filter	The number of dynamic MAC filters applied to the port.

Examples

The following example displays information about the 802.1X configuration.

```
device# show dot1x configuration
PAE Capability                : Authenticator Only
system-auth-control           : Enable
Number of Ports enabled       : 3
Re-Authentication             : Disabled
Authentication-fail-action    : Per Port
Mac Session Aging             : Enabled
Mac Session max-age           : 120 seconds
Protocol Version              : 1
quiet-period                  : 60 Seconds
tx-period                     : 30 Seconds
supptimeout                   : 30 Seconds
servertimeout                 : 30 Seconds
maxreq                        : 2
reAuthmax                     : 2
re-authperiod                 : 3600 Seconds
global strict security        : Enable
```

The following example displays information about the 802.1X configuration on an individual port.

```
device# show dot1x configuration ethernet 4/1/12
Port-Control                  : control-auto
filter strict security        : Enable
Action on RADIUS timeout      : Restart authentication
Authentication-fail-action    : Restricted VLAN(299)
PVID State                    : Normal (1)
Original PVID                 : 1
Authorized PVID ref count     : 2
Restricted PVID ref count     : 0
Radius assign PVID ref count  : 0
num mac sessions              : 2
num mac authorized            : 2
num Dynamic Tagged Vlan       : 0
Number of Auth filter         : 0
```

show dot1x mac-address-filter

Displays the MAC address filters active on the device.

Syntax

show dot1x mac-address-filter [**all** | **ethernet** *slot/port* | **user-defined**]

Parameters

all

Displays dynamically applied MAC address filters active on the device.

ethernet *slot/port*

Displays dynamically applied MAC address filters active on an interface.

user-defined

Displays user-defined MAC address filters active on the device.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

dot1x configuration mode

Examples

The following example displays dynamically applied MAC address filters active on an interface.

```
device# show dot1x mac-address-filter ethernet 1/3
Port 1/3 MAC Address Filter information:
802.1X Dynamic MAC Address Filter :
mac filter-group 2
Port default MAC Address Filter:
No mac address filter is set
```

show dot1x mac-filter

Shows the layer 2 ACLs for 802.1X authentication.

Syntax

show dot1x mac-filter { **all** | **ethernet** *device/slot/port* }

Parameters

all

Specifies the ACLs at the global level.

ethernet *device/slot/port*

Specifies the ACLs at the interface level.

Modes

Global configuration

Interface configuration

Usage Guidelines

Command Output

The **show mac-filter** command displays the following information:

Output field	Description
Dynamic MAC filter-list	The MAC filter defined on the device.

Examples

The **show dot1x mac-filter** command displays the following information

```
device# show dot1x mac-filter all
802.1x MAC Address Filter information:
Port 1/1/48:
Dynamic MAC filter-list: 1
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x mac-session

Displays information about the dot1x-MAC-session on each port on the device.

Syntax

show dot1x mac-sessions [**brief** | **ip-addr**]

Parameters

brief

Displays information about the dot1x-MAC-sessions in brief.

ip-addr

Displays dot1x-mac-session information with an IP address instead of a MAC address.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

dot1x configuration mode

Command Output

The **show dot1x mac-sessions** command displays the following information:

Output field	Description
Port	The port on which the dot1x-MAC-session exists.
MAC/IP (username)	The MAC address of the client and the username used for RADIUS authentication.
Vlan	The VLAN to which the port is currently assigned.
Auth-State	The authentication state of the dot1x-MAC-session. This can be one of the following states: • permit - The client has been successfully authenticated, and traffic from the client is being forwarded normally. • blocked - Authentication failed for the client, and traffic from the client is being dropped in hardware. • restricted - Authentication failed for the client, but traffic from the client is allowed in the restricted VLAN only. • init - The client is in is in the process of 802.1X authentication, or has not started the authentication process.
Age	The software age of the dot1x-MAC-session.

Output field	Description
PAE State	The current status of the Authenticator PAE state machine. This state can be INITIALIZE, DISCONNECTED, CONNECTING, AUTHENTICATING, AUTHENTICATED, ABORTING, HELD,FORCE_AUTH, or FORCE_UNAUTH. **NOTE** When the Authenticator PAE state machine is in the AUTHENTICATING state, if the reAuthenticate, eapStart, eapLogoff, or authTimeout parameters are set to TRUE, it may place the Authenticator PAE state machine indefinitely in the ABORTING state. If this should happen, use the **dot1x initialize** command to initialize 802.1X authentication on the port, or unplug the client or hub connected to the port, then reconnect it.

The **show dot1x mac-session brief** command displays the following information:

Output field	Description
Port	Information about the users connected to each port.
Number of users	The number of users connected to the port.
Number of Authorized users	The number of users connected to the port that have been successfully authenticated.
Dynamic VLAN	Whether the port is a member of a RADIUS-specified VLAN.
Dynamic ACL	Whether RADIUS-specified IP ACLs are applied to the port.
Dynamic MAC-Filter	Whether RADIUS-specified MAC address filters are applied to the port.

Examples

The following example displays information about the dot1x-MAC-session on each port on the device.

```
device# show dot1x mac-session
Port MAC/IP(username)           Vlan       Auth      ACL      Age    PAE
State State
-------------------------------------------------------------------------------
4/1/12 0044.0002.0002 :user1    10         permit    none     Ena    AUTHENTICATED
4/1/12 0044.0002.0003 :user2    10         permit    none     Ena    AUTHENTICATED
```

The following example displays information about the dot1x-MAC-session in brief.

```
device# show dot1x mac-session brief
Port           Number of    Number of           Dynamic     Dynamic   Dynamic
               users        Authorized users    VLAN        ACL       MAC-Filt
-----------------------------------------------------------------------
4/1/12         2            2                    no          no        no
```

show dot1x sessions

Shows 802.1X authentication sessions at the global and interface level.

Syntax

show dot1x sessions { **all** | **brief** | **ethernet** *unit/slot/port* }

Parameters

all

Specifies the 802.1X authentication sessions for all ports.

brief

Specifies details of 802.1X authentication sessions in brief.

ethernet *unit/slot/port*

Specifies the 802.1X authentication sessions of an interface.

Modes

Privileged EXEC mode

Global configuration

Interface configuration

Authentication configuration mode

Command Output

The **show dot1x sessions** command displays the following information:

Output field	Description
Port	The port number.
MAC Address	The MAC address of the client.
IP Address	The IP address of the client. The IP address of the authenticated host is displayed only if an IP ACL is applied to the interface based on the RADIUS server response.
VLAN	The VLAN
Auth State	The authentication state.
ACL	The specific ACL applied.
Age	The age of the session.
PAE State	The Port Access Entity state.

Examples

The following example displays 802.1X sessions for all interfaces.

```
device(config)# show dot1x sessions all
-------------------------------------------------------------------------------
Port    MAC             IP          User    Vlan  Auth     ACL     Age   PAE
        Addr            Addr                      State                  State
-------------------------------------------------------------------------------
2/1/1   0010.9400.1303  192.85.1.2   User1  200   permit  in-102  Ena   AUTHENTICATED
2/1/1   0010.9400.1304  1.1.1.4      User2  2009  permit  in-102  Ena   AUTHENTICATED
2/1/1   0010.9400.1305  1.1.1.2      User3  2009  permit  in-102  Ena   AUTHENTICATED
2/1/1   0010.9400.1306  1.1.1.6      User4  2009  permit  in-102  Ena   AUTHENTICATED
```

The following example displays 802.1X authentication sessions for a specified interface.

```
device(config)# show dot1x sessions all
-------------------------------------------------------------------------------
Port    MAC             IP          User    Vlan  Auth     ACL     Age   PAE
        Addr            Addr                      State                  State
-------------------------------------------------------------------------------
2/1/1   0010.9400.1303  192.85.1.2   User1  200   permit  in-102  Ena   AUTHENTICATED
2/1/1   0010.9400.1304  1.1.1.4      User2  2009  permit  in-102  Ena   AUTHENTICATED
2/1/1   0010.9400.1305  1.1.1.2      User3  2009  permit  in-102  Ena   AUTHENTICATED
2/1/1   0010.9400.1306  1.1.1.6      User4  2009  permit  in-102  Ena   AUTHENTICATED
```

The following example displays 802.1X authentication sessions brief.

```
device# show dot1x sessions brief
-------------------------------------------------------------------------
Port    Number of  Number of   Number of  Untagged          Dynamic   Dynamic
        Attempted  Authorized  Denied     VLAN Type         Port ACL  MAC-Filt
        Users      Users       Users
-------------------------------------------------------------------------
1/1/2   1          1           0           Radius-VLAN       No        No
1/1/3   0          0           0           Auth-Default-VLAN No        No
1/1/4   0          0           0           Auth-Default-VLAN No        No
1/1/5   0          0           0           Auth-Default-VLAN No        No
2/1/1   0          0           0           Auth-Default-VLAN No        No
2/1/2   0          0           0           Auth-Default-VLAN No        No
2/1/4   0          0           0           Auth-Default-VLAN No        No
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x statistics

Displays the 802.1X authentication statistics.

Syntax

show dot1x statistics { **all** | **ethernet** *device/slot/port* }

Parameters

all

Displays the 802.1X authentication statistics for all interfaces.

ethernet *device/slot/port*

Displays the 802.1X authentication statistics for the specified interface.

Modes

Privileged EXEC mode

Global configuration

Interface configuration

Authentication configuration mode

Usage Guidelines

Command Output

The **show dot1x statistics** command displays the following information:

Output field	Description
RX EAPOL Start	The number of EAPOL-Start frames received on the port.
RX EAPOL Logoff	The number of EAPOL-Logoff frames received on the port.
RX EAPOL Invalid	The number of invalid EAPOL frames received on the port.
RX EAPOL Total	The total number of EAPOL frames received on the port.
RX EAP Resp/Id	The number of EAP-Response/Identity frames received on the port
RX EAP Resp other than Resp/Id	The total number of EAP-Response frames received on the port that were not EAP-Response/Identity frames.
RX EAP Length Error	The number of EAP frames received on the port that have an invalid packet body length.
Last EAPOL Version	The version number of the last EAPOL frame received on the port.
Last EAPOL Source	The source MAC address in the last EAPOL frame received on the port.
TX EAPOL Total	The total number of EAPOL frames transmitted on the port.
TX EAP Req/Id	The number of EAP-Request/Identity frames transmitted on the port.
TX EAP Req other than Req/Id	The number of EAP-Request frames transmitted on the port that were not EAP-Request/Identity frames.

Examples

The following example displays 802.1X authentication statistics for port 10/2/1.

```
device# show dot1x statistics ethernet 10/2/1

Port 10/2/1 Statistics:
RX EAPOL Start : 2
RX EAPOL Logoff : 2
RX EAPOL Invalid : 0
RX EAPOL Total : 12
RX EAP Resp/Id : 4
RX EAP Resp other than Resp/Id : 4
RX EAP Length Error : 0
Last EAPOL Version : 1
Last EAPOL Source : 0022.0002.0002
TX EAPOL Total : 0
TX EAP Req/Id : 10417
TX EAP Req other than Req/Id : 2
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka config

Shows the MACsec Key Agreement (MKA) configuration for the device.

Syntax

show dot1x-mka config

Modes

EXEC or Privileged EXEC mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

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 *device/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 for MACsec transmissions on the named group is set at this value.
macsec cipher-suite gcm-aes-128 or macsec cipher-suite gcm-aes-128 integrity-only	MACsec encryptions between members of the group are encrypted. or ICV checking only is performed, but no encryption is performed.
macsec confidentiality-offset *value*	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 }	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.
key *value* 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.
enable ethernet *device/slot/port* mka-cfg-group *name* key *hexadecimal value* name *hexadecimal value*	The specified interface is enabled for MACsec. The interface belongs to the named MKA group, and the interface uses the pre-shared key shown to confirm peers with which it can communicate.

Examples

The following example displays MACsec configuration information for an ICX 6610 device with MACsec enabled. Two MKA groups, test1 and group1, are configured. Interfaces with either group of parameters applied could form secure channels because the groups have the same pre-shared key.

```
device(config-dot1x-mka-1/3/2)# show dot1x-mka config

dot1x-mka-enable
 mka-cfg-group test1
  key-server-priority 5
  macsec cipher-suite gcm-aes-128 integrity-only
  macsec confidentiality-offset 30
  macsec frame-validation strict
mka-cfg-group group1
  key-server-priority 20
  macsec cipher-suite gcm-aes-128
  macsec confidentiality-offset 30
 enable-mka ethernet 1/3/2
  mka-group test1
  pre-shared-key 135bd758 b0ee5c11 c55ff6ab 19fdb199 key-name 96437a93 ccf10d9d fe347846 cce52c7d
 enable-mka ethernet 1/3/3
  mka-group group1
  pre-shared-key 135bd758 b0ee5c11 c55ff6ab 19fdb199 key-name 96437a93 ccf10d9d fe347846 cce52c7d
 enable-mka ethernet 1/3/4
  mka-group group1
  pre-shared-key 135bd758 b0ee5c11 c55ff6ab 19fdb199 key-name 96437a93 ccf10d9d fe347846 cce52c7d
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka config-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 config-group *group-name*

Parameters

group-name Limits the group configuration displayed to the named MKA group.

Modes

EXEC or Privileged EXEC mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

Command Output

The **show dot1x-mka config-group** command displays the following information:

Output field	Description
mka-cfg-group	The configuration details that follow are for the specified MACsec MKA group.
key-server-priority	The key-server priority for MACsec transmissions on the named group is set at te specified value.
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.

Examples

The following example lists the configuration details for MKA group test1.

```
device(config-dot1x-mka-1/3/2)# show dot1x-mka config-group test1

mka-cfg-group test1
  key-server-priority 5
  macsec cipher-suite gcm-aes-128 integrity-only
  macsec confidentiality-offset 30
  macsec frame-validation check
        macsec replay-protection strict
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka sessions

Displays a summary of all MACsec Key Agreement (MKA) sessions on the device.

Syntax

show dot1x-mka sessions brief

show dot1x-mka sessions ethernet *device/slot/port*

Parameters

brief Displays a brief status of all MKA sessions.

ethernet *device/slot/port* Displays MKA sessions that are active on a specified Ethernet interface. The Ethernet interface is specified by device position in stack, slot on the device, and interface on the slot.

Modes

EXEC or Privileged EXEC mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

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 configured on the designated interface.

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.
MKA cfg group Name	The designated MKA configuration group has been applied to the designated interface.
DOT1X-MKA Enabled (Yes, No)	Indicates whether MACsec is enabled for the designated interface.
DOT1X-MKA Active (Yes, No)	Indicates whether MACsec is active on the interface.
Key Server (Yes, No)	Indicates whether the MACsec 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.

Output field	Description
Capability (Integrity and or confidentiality)	Indicates whether ICV checks are being performed on MACsec frames and whether encryption is being applied.
Desired (Yes, No)	Indicates whether port is interested in becoming the key-server.
Protection (Yes, No)	Indicates whether replay protection is applied to the interface.
Frame Validation (Yes, No)	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.
Key Server Priority (1 to 127)	Specifies the key-server priority configured on the interface.
Secure Channel Information	The following fields describe a secure channel established on this interface.
Local SCI	Provides the hexadecimal value of the Secure Channel Identifier for this channel.
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.
Latest SAK Status (RX and or TX)	Indicates the Secure Association Key (SAK) state.
Latest SAK AN	Provides the Association Number for the most recently active Secure Association Key.
Latest SAK KI	Provides the Key Identifier for the most recently active Secure Association Key.
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.)
Peer Information:	The output fields that follow provide information on actual and potential MACsec peer interfaces.
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

In the following example, all enabled MKA interfaces on the device are listed, along with configured parameters and current status.

```
device(config-dot1x-mka-1/3/2)# show dot1x-mka sessions brief

Port    Link-Status  MKA-Status  Key-Server  Negotiated Capability

1/3/2   Down         Pending     ---         ---
1/3/3   Up           Secured     No          Integrity, Confidentiality with Off. 30
1/3/4   Up           Secured     No          Integrity, Confidentiality with Off. 30
```

The following example lists MKA sessions that are active on Ethernet interface 1/3/3 (device 1, slot 3, port 3), with configuration details for each active interface.

```
device(config-dot1x-mka-1/3/3)# show dot1x-mka sessions ethernet 1/3/3

Interface                : 1/3/3

  MACsec Status          : Secured
  DOT1X-MKA Enabled      : Yes
  DOT1X-MKA Active       : Yes
  Key Server             : No

Configuration Status:
  Enabled                : Yes
  Capability             :  Integrity,  Confidentiality
  Desired                : Yes
  Protection             : Yes
  Frame Validation       : Disable
  Replay Protection      : Strict
  Replay Protection Size  : 0
  Cipher Suite           : GCM-AES-128
  Key Server Priority    : 20

  Local SCI              : 748ef8344a510082
  Member Identifier      : 802ed0536fcafc43407ba222
  Message Number         : 8612

Secure Channel Information:
  Latest SAK Status      : Rx & Tx
  Latest SAK AN          : 0
  Latest KI              : d08483062aa9457e7c2470e300000001
  Negotiated Capability  : Integrity, Confidentiality with offset 30

Peer Information:
State        Member Identifier          Message Number    SCI                Priority
-----        -----------------          --------------    ----------------   --------
Live         d08483062aa9457e7c2470e3             8527    748ef83443910082         20
```

History

Release version	Command history
08.0.20	This command was introduced.

show dot1x-mka statistics

Displays current MACsec Key Agreement (MKA) statistics on the interface.

Syntax

show dot1x-mka statistics ethernet *device/slot/port*

Parameters

ethernet *device/slot/port*

Ethernet interface for which MKA statistics are to be displayed. The interface is designated by a device number in stack/slot on the device/interface on the slot.

Modes

EXEC or Privileged EXEC mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

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 (device/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
Number of SAK	Total number of SAKs received

Examples

The following example shows MKA statistics for Ethernet interface 1/3/3 (device 1, slot 3, port 3), which is transmitting and receiving MACsec frames.

```
device(config-dot1x-mka-1/3/3)# clear dot1x-mka statistics ethernet 1/3/3
device(config-dot1x-mka-1/3/3)# show dot1x-mka statistics ethernet 1/3/3

Interface                : 1/3/3

MKA in Pkts              : 8585
MKA in SAK Pkts          : 1
MKA in Bad Pkts          : 0
MKA in Bad ICV Pkts      : 0
MKA in Mismatch Pkts     : 0
MKA out Pkts             : 8687
MKA out SAK Pkts         : 0
Number of SAK            : 1
```

History

Release version	Command history
08.0.20	This command was introduced.

show eee-statistics

Displays the global energy efficient statistics.

Syntax

show eee-statistics

Modes

Global configuration mode

Usage Guidelines

Command Output

The **show eee-statistics** command displays the following information:

Output field	Description
Port	The port number.
EEE-State	Displays if Energy Efficient Ethernet is enabled or disabled. If disabled then all the counters will be 0. If EEE is enabled, then these counters will be updated.
TXEventCount	TX EEE Low Power Idle (LPI) event counter. This counter specifies the number of times the LPI mode has been enforced by EEE on Transmit side.
TXDuration	TX EEE LPI duration counter. This is an LPI event duration counter on the transmit path which gets updated if the port is in LPI mode.
RXEventCount	RX EEE LPI event counter. This counter specifies the number of times the LPI mode has been enforced by EEE on the receive side.
RXDuration	RX EEE LPI duration counter. This is an LPI event duration counter on the receive path which gets updated if the port is in LPI mode.

Examples

The following example displays Energy Efficient Ethernet globally.

```
device# show eee-statistics
Port        EEE-State  TXEventCount       TXDuration        RXEventCount                RXDuration
1/1/1       Enable       0                    0                 0                          0
1/1/2       Enable       0                    0                 0                          0
1/1/3       Enable       17                 2551234             16                       2561886
1/1/4       Enable       17                 2545628             16                       50953524
1/1/5       Enable       2                  2550749             2                        50952549
1/1/6       Enable       1                  2543935             1                        2551760
1/1/7       Enable       17                 2549030             17                       2550750
1/1/8       Enable       2                  419455              16                       50952710
1/1/9       Enable       1                  424565              1                        50950470
1/1/10      Enable       17                 2549030             1                        2549101
1/1/11      Enable       2                  419455              2                        424563
1/1/12      Enable       1                  424565              10                       50945833
1/1/13      Enable       2                  1526709             10                       1532337
1/1/14      Enable       10                 1531808             2                        2561886
1/1/15      Enable       10                 1531391             2                        1531834
1/1/16      Enable       2                  1526292             10                       50945548
1/1/17      Enable       2                  1542560             10                       50957135
1/1/18      Enable       10                 1537443             2                        1542565
1/1/19      Enable       10                 1528600             2                        1533722
1/1/20      Enable       2                 1533717              10                       50948350
1/1/21      Enable       2                 1533203              10                       50947920
1/1/22      Enable       10                 1528087             2                        1533230
1/1/23      Enable       10                 1527677             2                        1532799
1/1/24      Enable       2                 1532794              10                       50947596
```

History

Release version	Command history
08.0.30	This command was introduced.

show eee-statistics ethernet

Displays the Energy Efficient Ethernet statistics on a specific interface.

Syntax

show eee-statistics ethernet *stackid/slot/port*

Modes

Global configuration mode

Usage Guidelines

Command Output

The **show eee-statistics ethernet** command displays the following information:

Output field	Description
Port	The port number.
EEE-State	Displays if Energy Efficient Ethernet is enabled or disabled. If disabled then all the counters will be 0. If EEE is enabled, then these counters will be updated.
TXEventCount	TX EEE Low Power Idle (LPI) event counter. This counter specifies the number of times the LPI mode has been enforced by EEE on Transmit side.
TXDuration	The total time from the first LPI (Low Power Idle) signal transmission. This is an LPI event duration counter on the transmit path which gets updated if the port is in LPI mode.
RXEventCount	The LPI signal reception count. This counter specifies the number of times the LPI mode has been enforced by EEE on the receive side.
RXDuration	Total time from the first LPI signal reception. This is an LPI event duration counter on the receive path which gets updated if the port is in LPI mode.

Examples

The following example displays energy efficient statistics on a specific interface.

```
device(config)# show eee-statistics ethernet 1/1/4

Port      EEE-State       TXEventCount       TXDuration        RXEventCount        RXDuration
1/1/4      Enable           17                  2545628            16                  50953524
```

History

Release version	Command history
08.0.30	This command was introduced.

show errdisable

Displays information about errdisabled ports.

Syntax

show errdisable { **recovery** | **summary** }

Parameters

recovery

Displays all the default error disable recovery states for all possible conditions.

summary

Displays the port number along with the reason why the port is in an errdisable state and the method used to recover the port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

Examples

The following example shows the errdisable recovery information.

```
device# show errdisable recovery
ErrDisable Reason                                                    Timer Status
---------------------------------------------------------------------------------
all reason                                                           Enabled
bpduguard                                                            Enabled
loopDetection                                                        Enabled
invalid license                                                      Disabled
packet-inerror                                                       Enabled
Reload the switch or stack to enable this port in 10G speed          Disabled
stack-port-resiliency                                                Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
                                                                     Disabled
loam-critical-event                                                  Disabled
                                                                     Disabled
                                                                     Disabled

Timeout Value: 300 seconds
PoD Timeout Value: 30 seconds

Interface that will be enabled at the next timeout:

Interface         Errdisable reason   Time left (sec)

--------------    -----------------   ---------------
```

The following example shows the errdisable summary information. In this example, port 6 is errdisabled for a BPDU guard violation.

```
device# show errdisable summary
Port 6 ERR_DiSABLED for bpduguard
```

show ethernet loopback interfaces

Displays the status and details of each Ethernet loopback-enabled port and the associated VLANs.

Syntax

show ethernet loopback interfaces [**brief** | **port** *stackid/slot/port* | **vlan** *vlan-id*]

Parameters

brief

Displays the Ethernet loopback information in brief mode.

port

Displays the status and details of each port.

stackid/slot/port

Specifies the port number.

vlan

Displays the status and details of a VLAN.

vlan-id

Specifies the VLAN ID.

Modes

Privileged EXEC mode

Global configuration mode

VLAN configuration mode

Command Output

The **show ethernet loopback interfaces** command displays the following information:

Output field	Description
Interface Type	Type of interface (VLAN-aware or VLAN-unaware)
Interface Port	Interface ID (Port number)
Interface Mode	Flow classification mode (Flow-aware or Flow-unaware)
Flow Mode DA/SA	Destination and Source MAC address of the flow

Examples

The following example shows the output of the **show ethernet loopback interfaces** command.

```
device(config-vlan-10)# show ethernet loopback interfaces

ETHERNET LOOPBACK INTERFACE [1/1/11] (In Service)
Interface Type  : PORT
Interface Port  : 1/1/11
Interface Mode  : FLOW-UNAWARE
Flow Mode DA/SA : ANY/ANY
```

The following example shows the output of the **show ethernet loopback interfaces brief** command.

```
device(config-vlan-10)# show ethernet loopback interfaces brief
PORT         TYPE  VLANS  STATUS  OP-MODE      D-MAC          S-MAC
==========|======|=====|========|=======|==============|==============
1/1/11     |  PORT|    0|    ACTV|FLOW-U |            ANY|            ANY
1/1/12     |  VLAN|    1|    ACTV|FLOW-A |1111.2222.3333|4444.5555.5555
```

The following example shows the output of the **show ethernet loopback interfaces port** command.

```
device(config-vlan-10)# show ethernet loopback interfaces port 1/1/1
ETHERNET LOOPBACK INTERFACE [1/1/1] (In Service)
Interface Type  : PORT
Interface Port  : 1/1/1
Interface Mode  : FLOW-UNAWARE
Flow Mode DA/SA : ANY/ANY
```

History

Release version	Command history
08.0.30	This command was introduced.

show ethernet loopback resources

Displays the available resources and the resources that are used by loopback testing.

Syntax

show ethernet loopback resources

Modes

Privileged EXEC mode

Global configuration mode

VLAN configuration mode

Command Output

The **show ethernet loopback resources** command displays the following information:

Output field	Description
Interface Resource	Maximum number of ports that can be enabled with Ethernet loopback.
H/W Pool Resource	Maximum hardware resource for loopback.

Examples

The following example shows the output of the **show ethernet loopback resources** command.

```
device(config)# show ethernet loopback resources
Ethernet Loopback Resource:
     RESOURCE NAME       MAX      USED    AVAILABLE
======================|========|========|===========
     Interface Resource|     20|       0|      20
     H/W Pool Resource|      40|       0|      40
```

History

Release version	Command history
08.0.30	This command was introduced.

show fdp entry

Displays the detailed Foundry Discovery Protocol (FDP) and Cisco Discovery Protocol (CDP) information for all neighbor devices or for a specific device.

Syntax

show fdp entry { * | *device-id* }

Parameters

*

Displays the detailed FDP updates for all neighbor devices.

device-id

Specifies the device ID of the FDP neighbor entry for which the update information has to be displayed. The value is an ASCII String.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show fdp entry** command displays the following information.

Output field	Description
Device ID	The hostname of the neighbor. In addition, this line lists the VLAN memberships and other VLAN information for the neighbor port that sent the update to this device.
Entry address(es)	The Layer 3 protocol addresses configured on the neighbor port that sent the update to this device. If the neighbor is a Layer 2 Switch, this field lists the management IP address.
Platform	The product platform of the neighbor.
Interface	The interface on which this device received an FDP or CDP update for the neighbor.
Port ID	The interface through which the neighbor sent the update.
Holdtime	The maximum number of seconds this device can keep the information received in the update before discarding it.
Version	The software version running on the neighbor.

Examples

The following is a sample output of the **show fdp entry** command.

```
device# show fdp entry FastIronB

Device ID: FastIronB configured as default VLAN1, tag-type8100
Entry address(es):
Platform: FastIron Router, Capabilities: Router
Interface: Eth 1/2/9
Port ID (outgoing port): Eth 1/2/9 is TAGGED in following VLAN(s):
9 10 11
Holdtime : 176 seconds
```

show fdp interface

Displays Foundry Discovery Protocol (FDP) information for an interface.

Syntax

show fdp interface [**ethernet** *stackid/slot/port*]

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet port ID in the format stacked/slot/port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show fdp interface** command displays the following information.

Output field	Description
Holdtime	The maximum number of seconds this device can keep the information received in the update before discarding it.

Examples

The following example shows information for ethernet port 1/2/3.

```
device# show fdp interface ethernet 1/2/3

FastEthernet1/2/3 is up, line protocol is up
Encapsulation ethernet
Sending FDP packets every 5 seconds
Holdtime is 180 seconds
```

show fdp neighbors

Displays the Cisco neighbors the Brocade device has learned from CDP packets.

Syntax

show fdp neighbors [**detail** | **ethernet** *stackid/slot/port*]

Parameters

detail

Displays detailed information for the neighbors.

ethernet *stackid/slot/port*

Specifies the Ethernet port ID in the format stacked/slot/port for which the information has to be displayed.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example shows a sample output of the **show fdp neighbors** command.

```
device# show fdp neighbors detail

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
(*) indicates a Cisco device
Device ID      Local Int    Holdtm   Capability  Platform     Port ID
-------------- ------------ ------   ----------  -----------  -------------
(*)Router      Eth 1/1/1      124      R          cisco RSP4   FastEthernet5/0/0
```

The following example shows a sample output of the **show fdp neighbors detail** command.

```
device# show fdp neighbors detail

Device ID: Router
Entry address(es):
            IP address: 10.95.6.143
Platform: cisco RSP4, Capabilities: Router
Interface: Eth 1/1/1, Port ID (outgoing port): FastEthernet5/0/0
Holdtime : 150 seconds
Version :
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-JSV-M), Version 12.0(5)T1, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 19-Aug-99 04:12 by cmong
```

The following example shows a sample output of the **show fdp neighbors ethernet** command.

```
device# show fdp neighbors ethernet 1/1/5

Device ID: Router
Entry address(es):
IP address: 10.95.6.143
Platform: cisco RSP4, Capabilities: Router
Interface: Eth 1/1/5, Port ID (outgoing port): FastEthernet5/0/0
Holdtime : 127 seconds
Version :
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-JSV-M), Version 12.0(5)T1, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 19-Aug-99 04:12 by cmong
```

show fdp traffic

Displays Foundry Discovery Protocol (FDP) and Cisco Discovery Protocol (CDP) packet statistics.

Syntax

show fdp traffic

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example shows a sample output of the **show fdp traffic** command.

```
device# show fdp traffic

CDP/FDP counters:
Total packets output: 6, Input: 3
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid packet: 0, Fragmented: 0
Internal errors: 0
```

show files

Displays the list of files in the flash memory.

Syntax

show files [*dir-name*]

Parameters

dir-name

Specifies the directory name.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example is a sample output of the **show files** command.

```
device# show files

Type    Size        Name
-----------------------
F         28203908     primary
F         27949956     secondary
F         641         startup-config.txt
F         391         stacking.boot
F         76942         debug.boot
F         638         startup-config.backup
F         0             startup-config.no

        56232476 bytes 7 File(s) in FI root

        1771020288 bytes free in FI root
        1771020288 bytes free in /
```

show files disk0

Displays the contents of the USB flash drive.

Syntax

show files disk0

Parameters

Modes

Enable mode

Usage Guidelines

Insert the flash drive in the device and enter the **show files disk0** command to display the contents of the USB flash drive.

Examples

The following example displays the contents of the USB flash drive.

```
device# show files disk0
F             681 20140611132829945ICX7450-PREM-LIC-SW.XML
F        28483780 SPS08030q066.bin
F             391 stacking.boot
F               0 sil_logs
F        28483780 pri.bin
F             391 stacking.boot1111
F            2160 running-configsp2
F            2162 startup-config.sp2
F            2160 run1
F            5344 core-file
```

History

Release version	Command history
08.0.30	This command was introduced.

show flash

Displays flash memory contents on the device.

Syntax

show flash [**unit** *unit-num*]

Parameters

unit *unit-num*

Displays flash memory contents for the specified stack unit.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

All configuration modes

Command Output

The **show flash** command displays the following information:

Output field	Description
Compressed Pri Code size	The flash code version installed on the primary flash area.
Compressed Sec Code size	The flash code version installed in the secondary flash area.
Compressed Boot-Monitor Image size	The boot code version installed in flash memory.

Usage Guidelines

Use this command to view the flash and boot images installed on the device.

The device does not have separate primary and secondary flash areas for the boot image. The flash memory module contains only one boot image.

Examples

The following example is a sample output of the **show flash** command.

```
device# show flash
Stack unit 1:
  Compressed Pri Code size = 28893380, Version:08.0.40T211 (SPS08040b074.bin)
  Compressed Sec Code size = 28893380, Version:08.0.40T211 (SPS08040b074.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.05T215
  Code Flash Free Space = 1779965952
```

show gvrp

Displays the GVRP information.

Syntax

show gvrp

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

GVRP configuration mode

Command Output

The **show gvrp** command displays the following information:

Output field	Description
Protocol state	The state of GVRP. The display shows one of the following: • GVRP is disabled on the system • GVRP is enabled on the system
GVRP BASE VLAN ID	The ID of the base VLAN used by GVRP.
GVRP MAX Leaveall Timer	The maximum number of milliseconds to which you can set the Leaveall timer.
GVRP Join Timer	The value of the Join timer.
GVRP Leave Timer	The value of the Leave timer.
GVRP Leave-all Timer	The value of the Leaveall timer.
Configuration that is being used	The configuration commands used to enable GVRP on individual ports. If GVRP learning or advertising is disabled on a port, this information also is displayed.
Spanning Tree	The type of STP enabled on the device. **NOTE** GVRP is only supported with Single STP.
Dropped Packets Count	The number of GVRP packets that the device has dropped. A GVRP packet can be dropped for either of the following reasons: • GVRP packets are received on a port on which GVRP is not enabled. **NOTE** If GVRP support is not globally enabled, the device does not drop the GVRP packets but instead forwards them at Layer 2. • GVRP packets are received with an invalid GARP protocol ID. The protocol ID must always be 0x0001.

Output field	Description
Number of VLANs in the GVRP Database	The number of VLANs in the GVRP database. **NOTE** This number includes the default VLAN (1), the GVRP base VLAN (4093), and the Single STP VLAN (4094). These VLANs are not advertised by GVRP but are maintained as "Registration Forbidden".
Maximum Number of VLANs that can be present	The maximum number of VLANs that can be configured on the device. This number includes statically configured VLANs, VLANs learned through GVRP, and VLANs 1, 4093, and 4094.

Examples

The following example displays sample output of the **show gvrp** command.

```
device# show gvrp
GVRP is enabled on the system
GVRP BASE VLAN ID : 4093
GVRP MAX Leaveall Timer : 300000 ms
GVRP Join Timer : 200 ms
GVRP Leave Timer : 600 ms
GVRP Leave-all Timer : 10000 ms
============================================================================
Configuration that is being used:
block-learning ethe 1/1/3
block-applicant ethe 1/2/7 ethe 1/2/11
enable ethe 1/1/1 to 1/1/7 ethe 1/2/1 ethe 1/2/7 ethe 1/2/11
============================================================================
Spanning Tree: SINGLE SPANNING TREE
Dropped Packets Count: 0
============================================================================
Number of VLANs in the GVRP Database: 15
Maximum Number of VLANs that can be present: 4095
============================================================================
```

show gvrp ethernet

Displays the GVRP information per individual port.

Syntax

show gvrp ethernet *stackid/slot/port*

Parameters

stackid/slot/port

Specifies the GVRP enabled ports.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

GVRP configuration mode

Command Output

The **show gvrp ethernet** command displays the following information:

Output field	Description
Port number	The port for which information is being displayed.
GVRP Enabled	Whether GVRP is enabled on the port.
GVRP Learning	Whether the port can learn VLAN information from GVRP.
GVRP Applicant	Whether the port can advertise VLAN information into GVRP.
Port State	The port link state, which can be UP or DOWN.
Forwarding	Whether the port is in the GVRP Forwarding state: • NO - The port is in the Blocking state. • YES - The port is in the Forwarding state.
VLAN Membership	The VLANs of which the port is a member. For each VLAN, the following information is shown: • VLAN ID - The VLAN ID. • Mode - The type of VLAN, which can be one of the following: • FIXED - The port will always be a member of this VLAN and the VLAN will always be advertised on this port by GVRP. A port becomes FIXED when you configure the port as a tagged member of a statically configured VLAN. • FORBIDDEN - The VLAN is one of the special VLANs that is not advertised or learned by GVRP. The following VLANs are forbidden: the default VLAN (1), the GVRP base VLAN (4093), or the Single STP VLAN (4094). • NORMAL - The port became a member of this VLAN after learning about the VLAN through GVRP. The port membership in the VLAN depends on GVRP. If the VLAN is removed from the ports that send GVRP advertisements to this device, then the port will stop being a member of the VLAN.

Examples

The following example shows GVRP information for an individual port.

```
device# show gvrp ethernet 1/2/1
Port 1/2/1 -
 GVRP Enabled   : YES
 GVRP Learning  : ALLOWED
 GVRP Applicant : ALLOWED
 Port State     : UP
 Forwarding     : YES

 VLAN Membership:        [VLAN-ID]            [MODE]
                                1          FORBIDDEN
                                2              FIXED
                             1001             NORMAL
                             1003             NORMAL
                             1004             NORMAL
                             1007             NORMAL
                             1009             NORMAL
                             1501             NORMAL
                             2507             NORMAL
                             4001             NORMAL
                             4093          FORBIDDEN
                             4094          FORBIDDEN
```

show gvrp statistics

Displays the GVRP statistics.

Syntax

show gvrp statistics { **all** | **ethernet** *stackid/slot/port* }

Parameters

all

Displays the GVRP statistics for all ports.

ethernet *stackid/slot/port*

Displays the GVRP statistics for a specific Ethernet port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

GVRP configuration mode

Command Output

The **show gvrp statistics ethernet** command displays the following information:

Output field	Description
Leave All Received	The number of Leaveall messages received.
Join Empty Received	The number of Join Empty messages received.
Join In Received	The number of Join In messages received.
Leave Empty Received	The number of Leave Empty messages received.
Leave In Received	The number of Leave In messages received.
Empty Received	The number of Empty messages received.
Leave All Transmitted	The number of Leaveall messages sent.
Join Empty Transmitted	The number of Join Empty messages sent.
Join In Transmitted	The number of Join In messages sent.
Leave Empty Transmitted	The number of Leave Empty messages sent.
Leave In Transmitted	The number of Leave In messages sent.
Empty Transmitted	The number of Empty messages sent.

Output field	Description
Invalid Messages/Attributes Skipped	The number of invalid messages or attributes received or skipped. This can occur in the following cases: • The incoming GVRP PDU has an incorrect length. • "End of PDU" was reached before the complete attribute could be parsed. • The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01). • The attribute that was being parsed had an invalid attribute length. • The attribute that was being parsed had an invalid GARP event. • The attribute that was being parsed had an invalid VLAN ID. The valid range is from 1 through 4095.
Failed Registrations	The number of failed registrations that have occurred. A failed registration can occur for the following reasons: • Join requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state). • An entry for a new GVRP VLAN could not be created in the GVRP database.

Examples

The following example shows the GVRP statistics for an individual port.

```
device# show gvrp statistics ethernet 1/2/1
PORT 1/2/1 Statistics:
 Leave All Received                    : 147
 Join Empty Received                   : 4193
 Join In Received                      : 599
 Leave Empty Received                  : 0
 Leave In Received                     : 0
 Empty Received                        : 588
 Leave All Transmitted                 : 157
 Join Empty Transmitted                : 1794
 Join In Transmitted                   : 598
 Leave Empty Transmitted               : 0
 Leave In Transmitted                  : 0
 Empty Transmitted                     : 1248
 Invalid Messages/Attributes Skipped   : 0
 Failed Registrations                  : 0
```

show gvrp vlan

Displays the GVRP VLAN information.

Syntax

show gvrp vlan { **all** | **brief** | *vlan-id* }

Parameters

all

Displays the information for all GVRP VLANs.

brief

Displays the GVRP VLAN information summary.

vlan-id

Displays the information for a specific VLAN ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

GVRP configuration mode

Command Output

The **show gvrp vlan brief** command displays the following information:

Output field	Description
Number of VLANs in the GVRP Database	The number of VLANs in the GVRP database. **NOTE** This number includes the default VLAN (1), the GVRP base VLAN (4093), and the Single STP VLAN (4094). These VLANs are not advertised by GVRP but are included in the total count.
Maximum Number of VLANs that can be present	The maximum number of VLANs that can be configured on the device. This number includes statically configured VLANs, VLANs learned through GVRP, and VLANs 1, 4093, and 4094.
VLAN-ID	The VLAN ID.
MODE	The type of VLAN, which can be one of the following: • STATIC - The VLAN is statically configured and cannot be removed by GVRP. This includes VLANs you have configured as well as the default VLAN (1), base GVRP VLAN (4093), and Single STP VLAN (4094). • DYNAMIC - The VLAN was learned through GVRP.
VLAN-INDEX	A number used as an index into the internal database.

The **show gvrp vlan** command displays the following information:

Output field	Description
VLAN-ID	The VLAN ID.
VLAN-INDEX	A number used as an index into the internal database.
STATIC	Whether the VLAN is a statically configured VLAN.
DEFAULT	Whether this is the default VLAN.
BASE-VLAN	Whether this is the base VLAN for GVRP.
Timer to Delete Entry Running	Whether all ports have left the VLAN and the timer to delete the VLAN itself is running.
Legend	The meanings of the letter codes used in other parts of the display.
Forbidden Members	The ports that cannot become members of a VLAN advertised or leaned by GVRP.
Fixed Members	The ports that are statically configured members of the VLAN. GVRP cannot remove these ports.
Normal (Dynamic) Members	The ports that were added by GVRP. These ports also can be removed by GVRP.
MODE	The type of VLAN, which can be one of the following: • STATIC - The VLAN is statically configured and cannot be removed by GVRP. This includes VLANs you have configured as well as the default VLAN (1), base GVRP VLAN (4093), and Single STP VLAN (4094). • DYNAMIC - The VLAN was learned through GVRP.

Examples

The following example shows the output of the **show gvrp vlan brief** command.

```
device# show gvrp vlan brief
Number of VLANs in the GVRP Database: 7
Maximum Number of VLANs that can be present: 4095

        [VLAN-ID]                          [MODE]       [VLAN-INDEX]

                1                  STATIC-DEFAULT                 0
                7                          STATIC                 2
               11                          STATIC                 4
             1001                         DYNAMIC                 7
             1003                         DYNAMIC                 8
             4093           STATIC-GVRP-BASE-VLAN                 6
             4094         STATIC-SINGLE-SPAN-VLAN                 5

================================================================================
```

The following example shows the output of the **show gvrp vlan** command.

```
device# show gvrp vlan 1001
VLAN-ID: 1001, VLAN-INDEX: 7, STATIC: NO, DEFAULT: NO, BASE-VLAN: NO
Timer to Delete Entry Running: NO
Legend: [S=Slot]
Forbidden Members: None
Fixed Members: None
Normal(Dynamic) Members: (S2) 1
```

show ignore-temp-shutdown

Displays the status of the ignore-temp-shutdown command. The status can be **Enabled** or **Disabled**.

Syntax

show ignore-temp-shutdown

Modes

Global configuration mode

Examples

```
device# show ignore-temp-shutdown
Global ignore temperature shutdown threshold mode status: Enabled

device# show ignore-temp-shutdown
Ignore temperature shutdown threshold mode unit1: Enabled/Disabled
Ignore temperature shutdown threshold mode unit2: Enabled/Disabled
Ignore temperature shutdown threshold mode unit3: Enabled/Disabled
Ignore temperature shutdown threshold mode unit4: Enabled/Disabled
                ..
                ..
Ignore temperature shutdown threshold mode unit12: Enabled/Disabled
```

History

Release version	Command history
8.0.30j	This command is newly introduced.

show inline power

Displays the inline power capacity, power allocation, power consumed and power priority details for all Power over Ethernet (PoE) ports.

Syntax

show inline power [*stack-unit* | **detail** | **pd** | *stack/slot/port*]

Parameters

stack-unit

Displays inline power information for the specified stack unit.

detail

Displays detailed information about the PoE power supplies installed in a PoE device.

pd

Displays inline power information for Powered Device (PD) ports, such as information about the number of PD ports available, how much PD power is available to Power Sourcing Equipment (PSE), how much PD power is currently switched to PSE, and the PD port level status.

stack/slot/port

Displays inline power information for a specific interface.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

Use this command to view power information details about PoE.

You can view the PoE operational status for the entire device, for a specific PoE module only, or for a specific interface only.

Command Output

The **show inline power** command displays the following information.

Output field	Description
Power Capacity	The total PoE power supply capacity and the amount of available power (current free) for PoE-power-consuming devices. Both values are shown in milliwatts.
Power Allocations	The number of times the device fulfilled PoE requests for power.
Port	The slot number and port number.

Output field	Description
Admin State	Specifies whether Power over Ethernet has been enabled on the port: • On: The **inline power** command was issued on the port. • Off: The **inline power** command has not been issued on the port.
Oper State	Shows the status of inline power on the port: • On: The PoE power supply is delivering inline power to the PD. • Off: The PoE power supply is not delivering inline power to the PD. • Non-PD: Identifies the ports connected to non powered devices. • Denied: The port is in standby mode (waiting for power) because the device does not currently have enough available power for the port. **NOTE** When you enable a port using the CLI, it may take 12 or more seconds before the operational state of that port is displayed correctly in the **show inline power** output.
Power Consumed	The number of current, actual milliwatts that the PD is consuming.
Power Allocated	The number of milliwatts allocated to the port. This value is either the default or configured maximum power level, or the power class that was automatically detected by the device.
PD Type	The type of PD connected to the port: • 802.3at: The PD connected to this port is 802.3at-compliant. • 802.3af: The PD connected to this port is 802.3af-compliant. • Legacy: The PD connected to this port is a legacy product (not 802.3af-compliant). • N/A: Power over Ethernet is configured on this port, and one of the following is true: – The device connected to this port is a nonpowered device. – No device is connected to this port. – The port is in standby or denied mode (waiting for power).
PD Class	Determines the maximum amount of power that a PD receives. This field can also be "Unknown," meaning that the device attached to the port cannot advertise its power class. **NOTE** If an 802.3at PD with a class 4 value is connected to a Brocade FastIron switch, the switch must be running FastIron release 08.0.20 or later to be able to perform the necessary power negotiations.
Pri	The port inline power priority, which determines the order in which the port receives power while in standby mode (waiting for power). Ports with a higher priority receive power before ports with a lower priority. This value can be one of the following: • 3: Low priority • 2: High priority • 1: Critical priority

Output field	Description
Fault/Error	If applicable, the fault or error that occurred on the port: • critical temperature: The PoE chip temperature limit rose above the safe operating level, thereby powering down the port. • detection failed: discharged capacitor - The port failed capacitor detection (legacy PD detection) because of a discharged capacitor. This can occur when connecting a non-PD on the port. • detection failed: out of range capacitor - The port failed capacitor detection (legacy PD detection) because of an out-of-range capacitor value. This can occur when connecting a non-PD on the port. • internal h/w fault: A hardware problem hindered port operation. • lack of power: The port shut down due to lack of power. • main supply voltage high: The voltage was higher than the maximum voltage limit, thereby tripping the port. • main supply voltage low: The voltage was lower than the minimum voltage limit, thereby tripping the port. • overload state: The PD consumed more power than the maximum limit configured on the port, based on the default configuration, user configuration, or CDP configuration. • over temperature: The port temperature rose above the temperature limit, thereby powering down the port. • PD DC fault: A succession of underload and overload states, or a PD DC/DC fault, caused the port to shut down. • short circuit: A short circuit was detected on the port delivering power. • underload state: The PD consumed less power than the minimum limit specified in the 802.3af standard. • voltage applied from ext src: The port failed capacitor detection (legacy PD detection) because the voltage applied to the port was from an external source.
Total	The total power in milliwatts being consumed by all PDs connected to the interface module, and the total power in milliwatts allocated to all PDs connected to the interface module.
Grand Total	The total number of current, actual milliwatts being consumed by all PDs connected to the PoE device, and the total number of milliwatts allocated to all PDs connected to the PoE device.

Examples

The following is sample output from the **show inline power** command.

```
device# show inline power

Power Capacity:        Total is 2160000 mWatts. Current Free is 18800 mWatts.
Power Allocations:     Requests Honored 769 times
... some lines omitted for brevity ...

Port   Admin Oper        --Power(mWatts)--       PD Type         PD Class     Pri    Fault/Error
             State State    Consumed     Allocated
-------------------------------------------------------------------------------
1/1/1     On          On        5070            9500            802.3af       n/a             3
n/a
1/1/2     On          On           1784            9500            Legacy           n/a
3         n/a
1/1/3     On          On           2347            9500            802.3af       n/a             3
n/a
1/1/4     On          On           2441            9500            Legacy           n/a
3      n/a
1/1/5     On          On           6667            9500            802.3af       Class 3      3
n/a
1/1/6     On          On           2723            9500            802.3af       Class 2      3
n/a
1/1/7  On          On           2347            9500            802.3af       n/a             3
n/a
1/1/8     On          On           2347            9500            802.3af       n/a             3
n/a
1/1/9     On          On           2347            9500            802.3af       n/a             3
n/a
1/1/10    On          On           4976            9500            802.3af       Class 3      3
n/a
1/1/11 On          On           4882            9500            802.3af       Class 3      3      n/a
1/1/12 On          On           4413            9500            802.3af       Class 1      3         n/a
1/1/13 On          On           7793            9500            802.3af       n/a             3
n/a
1/1/14    On          On           7512            9500            802.3af       n/a
3         n/a
1/1/15 On          On           8075            9500            802.3af       n/a             3
n/a
1/1/16    On          On           4131            9500            802.3af       Class 1      3
n/a
1/1/17 On    Non-PD    0         0      n/a        n/a       3   n/a
1/1/18 On    Non-PD    0         0      n/a        n/a       3   n/a
1/1/19 On    Off       0     30000      n/a        n/a       3   n/a
1/1/20 On    Off       0     30000      n/a        n/a       3   n/a
1/1/21 On    Non-PD    0         0      n/a        n/a       3   n/a
1/1/22 On    Non-PD    0         0      n/a        n/a       3   n/a
1/1/23 On    Non-PD    0         0      n/a        n/a       3   n/a
1/1/24 On    Non-PD    0         0      n/a        n/a       3   n/a
-------------------------------------------------------------------------------
Total                     137367         242000
... some lines omitted for brevity...
Grand Total             1846673        2127400
```

The following is sample output from the **show inline power pd** command.

```
device# show inline power pd

Number of PD Ports: 2
Total PD Power Available to PSE: 22400
Total PD Power Switched to PSE: 22400
Port      Oper       Oper        Fault/
             State      Mode        Error
---------------------------------
1/1/4  on      Legacy   n/a
1/2/1     On            802.3at     n/a
```

The following is sample output from the **show inline power detail** command.

```
device# show inline power detail

Power Supply Data On stack 1:
++++++++++++++++++
Power Supply #1:
        Max Curr:    7.5 Amps
        Voltage:    54.0 Volts
        Capacity:    410 Watts
        POE Details Info. On Stack 1 :
General PoE Data:
++++++++++++++++++
Firmware
Version
--------
02.1.0
Cumulative Port State Data:
++++++++++++++++++++++++++
#Ports    #Ports           #Ports       #Ports           #Ports            #Ports             #Ports
Admin-On     Admin-Off     Oper-On      Oper-Off      Off-Denied     Off-No-PD       Off-Fault
-------------------------------------------------------------------------------
45                  3                    0               48                 0
45                   0
Cumulative Port Power Data:
++++++++++++++++++++++++++
#Ports       #Ports       #Ports          Power               Power
Pri: 1       Pri: 2       Pri: 3          Consumption    Allocation
-----------------------------------------------------------
0               0              45                0.0 W               0.0 W
Power Supply Data On stack 2:
++++++++++++++++++
Power Supply Data:
++++++++++++++++++
Power Supply #1:
        Max Curr:    7.5 Amps
        Voltage:    54.0 Volts
        Capacity:    410 Watts
POE Details Info. On Stack 2 :
General PoE Data:
++++++++++++++++++
Firmware
Version
--------
02.1.0
Slot     #Ports      #Ports      #Ports      Power               Power              Power
            Pri: 1      Pri: 2      Pri: 3      Consumption   Allocation      Budget
-------------------------------------------------------------------------
3           0              0              48             513.468 W        739.200 W       65535.0 W
4           0              0              48             1349.320 W        1440.0 W       65535.0 W
-------------------------------------------------------------------------
Total:    0        0        96        1862.788 W    2179.200 W    131070.0 W
Cumulative Port State Data:
++++++++++++++++++++++++++
#Ports           #Ports           #Ports      #Ports           #Ports             #Ports
#Ports
Admin-On      Admin-Off     Oper-On     Oper-Off      Off-Denied      Off-No-PD      Off-Fault
-------------------------------------------------------------------------------
20                  4                  0              24                  0
20                  0
Cumulative Port Power Data:
++++++++++++++++++++++++++
#Ports       #Ports        #Ports        Power               Power
Pri: 1       Pri: 2        Pri: 3        Consumption   Allocation
-----------------------------------------------------------
20             0               0               0.0 W              0.0 W
Power Supply Data On stack 3:
++++++++++++++++++
Power Supply #1:
        Max Curr:    7.5 Amps
        Voltage:    54.0 Volts
```

```
        Capacity:    410 Watts
POE Details Info. On Stack 3 :
General PoE Data:
+++++++++++++++++
Firmware
Version
--------
02.1.0
Cumulative Port State Data:
+++++++++++++++++++++++++++
#Ports            #Ports           #Ports       #Ports           #Ports            #Ports
#Ports
Admin-On       Admin-Off     Oper-On   Oper-Off      Off-Denied     Off-No-PD      Off-Fault
-------------------------------------------------------------------------------
22                   2                  0               24                  0
22                    0
Cumulative Port Power Data:
+++++++++++++++++++++++++++
#Ports       #Ports      #Ports       Power             Power
Pri: 1       Pri: 2      Pri: 3       Consumption  Allocation
-------------------------------------------------
0              10             12             0.0 W             0.0 W
```

show interfaces ethernet

Displays Ethernet interface information.

Syntax

show interfaces ethernet *stackid/slot/port*

Parameters

stackid / slot / port

Stack ID number, slot number, and port number for an existing Ethernet interface.

Modes

Privileged EXEC mode

Examples

This example shows detailed interface information. Note that the priority flow control (PFC) is shown as enabled and information for the unicast and multicast egress queues is shown separately.

```
device# show interfaces ethernet 1/1/22

10GigabitEthernet1/1/22 is up, line protocol is up
  Port up for 16 minutes 1 seconds
  Hardware is 10GigabitEthernet, address is aabb.ccdd.ef14 (bia aabb.ccdd.ef14)
  Configured speed 10Gbit, actual 10Gbit, configured duplex fdx, actual fdx
  Member of 1 L2 VLANs, port is tagged, port state is FORWARDING
  BPDU guard is Disabled, ROOT protect is Disabled, Designated protect is Disabled
  Link Error Dampening is Disabled
  STP configured to ON, priority is level0, mac-learning is enabled
  ….
  …..
  MTU 1500 bytes
  Priority-Flow-Control is Enabled
  300 second input rate: 37014512 bits/sec, 9036 packets/sec, 0.38% utilization
  300 second output rate: 731174584 bits/sec, 178509 packets/sec, 7.58% 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
  26055807 packets output, 13340529672 bytes, 0 underruns
  Transmitted 0 broadcasts, 98 multicasts, 26055709 unicasts
  0 output errors, 0 collisions
  Relay Agent Information option: Disabled

UC Egress queues:
Queue counters    Queued packets    Dropped Packets
         0                 0             2074860
         1           2349160             2074861
         2           2349163             2074861
         3           2349165             2074860
         4           2349163             2074860
         5           2349165             2074860
         6           5461694              518651
         7           6498353                   0


MC Egress queues:
Queue counters    Queued packets    Dropped Packets
         0                 0                   0
         1                 0                   0
         2                 0                   0
         3                 0                   0
         4                 0                   0
```

This example shows information for an interface that has an ingress profile and an egress profile attached to a port.

```
device(config-if-e40000-1/1/1)# show interfaces ethernet 1/1/1

40GigabitEthernet1/1/1 is up, line protocol is up
  Port up for 5 days 12 hours 45 minutes 48 seconds
  Hardware is 40GigabitEthernet, address is 748e.f8f9.3d80 (bia 748e.f8f9.3d80)
  Configured speed 40Gbit, actual 40Gbit, configured duplex fdx, actual fdx
  Configured mdi mode AUTO, actual none
  Member of 1 L2 VLANs, port is tagged, port state is FORWARDING
  BPDU guard is Disabled, ROOT protect is Disabled, Designated protect is Disabled
  Link Error Dampening is Disabled
  STP configured to ON, priority is level0, mac-learning is enabled
  Flow Control is enabled
  Mirror disabled, Monitor disabled
  Mac-notification is disabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  IPG MII 96 bits-time, IPG GMII 96 bits-time
  MTU 1500 bytes, encapsulation ethernet
  Ingress Profile is i1
  Egress Profile is e1
  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
  8060797794 packets input, 1031782117647 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts, 8060797794 unicasts
  4 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  8078157201 packets output, 1034004121728 bytes, 0 underruns
  Transmitted 0 broadcasts, 0 multicasts, 8078157201 unicasts
  0 output errors, 0 collisions
  Relay Agent Information option: Disabled
```

This example shows information for the configured bandwidth on a specific interface. In this example the configured interface bandwidth value is 2000 kilobits.

```
device# show interfaces ethernet 1/1/1

GigabitEthernet1/1/1 is disabled, line protocol is down
  STP Root Guard is disabled, STP BPDU Guard is disabled
  Hardware is GigabitEthernet, address is 748e.f82a.6a00 (bia 748e.f82a.6a00)
  Configured speed auto, actual unknown, configured duplex fdx, actual unknown
Interface bandwidth is 2000 kbps
```

History

Release version	Command history
8.0.20	This command was modified to include PFC status and separate unicast and multicast egress queues.
8.0.30	This command was modified to include configured bandwidth status.

show interfaces tunnel

Displays tunnel interface information.

Syntax

show interfaces tunnel *tunnel-number*

Parameters

tunnel-number

Specifies the tunnel number. Valid values range from 1 through 72,

Modes

Privileged EXEC mode

Command Output

The **show interfaces tunnel** command displays the following information:

Field	Definition
Hardware is Tunnel	The interface is a tunnel interface.
Tunnel source	The source address for the tunnel.
Tunnel destination	The destination address for the tunnel.
Tunnel mode	The tunnel mode. The gre specifies that the tunnel will use GRE encapsulation (IP protocol 47).
Interface bandwidth	The configured bandwidth on a tunnel interface for routing metric purposes only.
Port name	The port name (if applicable).
Internet address	The internet address.
MTU	The configured path maximum transmission unit.
encapsulation GRE	GRE encapsulation is enabled on the port.
Keepalive	Indicates whether or not GRE link keepalive is enabled.
Path MTU Discovery	Indicates whether or not PMTUD is enabled. If PMTUD is enabled, the MTU value is also displayed.
Path MTU	The PMTU that is dynamically learned.
Age-timer	Indicates the pmtd aging timer configuration in minutes.The default is 10. The range is from 10 - 30.
Path MTU will expire	Indicates the time after which the learned PMTU expires. This line is displayed only when a PMTU is dynamically learned.

Examples

This example displays the GRE tunnel configuration and the pmtd aging timer information..

```
show interfaces tunnel 10
Tunnel10 is up, line protocol is up
  Hardware is Tunnel
  Tunnel source  10.1.41.10
  Tunnel destination is 10.1.14.10
  Tunnel mode gre ip
  Port name is GRE_10_to_VR1_on_FCX_STACK
  Internet address is 10.11.1.1/31, MTU 1476 bytes, encapsulation GRE
  Keepalive is not Enabled
  Path MTU Discovery: Enabled, MTU is 1428 bytes, age-timer: 10 minutes
  Path MTU will expire in 0 minutes 50 secs
```

This example shows information for the configured interface bandwidth value on a tunnel interface.

```
device# show interfaces tunnel 2

Tunnel2 is up, line protocol is up
  Hardware is Tunnel
  Tunnel source  10.70.15.1
  Tunnel destination is 10.70.15.2
  Tunnel mode gre ip
  Interface bandwidth is 2000 kbps
  No port name
  Internet address is: 10.0.0.1/24
  Tunnel TOS 0, Tunnel TTL 255, Tunnel MTU 1476 bytes
  Keepalive is not Enabled

  Tunnel Packet Statistics:
                              Unicast Packets                    Multicast Packets
       In-Port(s)     [Rcv-from-tnnl    Xmit-to-tnnl]     [Rcv-from-tnnl    Xmit-to-tnnl]
       e1/1 - e1/24   2224              0                 0                 0
```

History

Release version	Command history
8.0.30	This command was modified to include configured bandwidth status.

show interfaces ve

Displays Virtual Ethernet (VE) interface information.

Syntax

show interfaces ve *vlan_id*

Parameters

vlan_id

Specifies the configured corresponding VLAN interface.

Modes

Privileged EXEC mode

Examples

This example shows information for the configured bandwidth on a VE interface. In this example the configured interface bandwidth value is 2000 kilobits.

```
device#show interfaces ve 100
Ve100 is up, line protocol is up
  Type is Vlan (Vlan Id: 100)
  Hardware is Virtual Ethernet, address is 748e.f82a.cf00 (bia 748e.f82a.cf00)
  No port name
  Vlan id: 100
  Interface bandwidth is 2000 kbps
 ipv6 address 190::1/64
```

History

Release version	Command history
8.0.30	This command was modified to include configured bandwidth status.

show ip access-lists

Displays IPv4 access list information.

Syntax

show ip access-lists [*acl-num* | *acl-name*]

Parameters

acl-num

Displays the information for the ACL with the specified ACL number.

acl-name

Displays information for the ACL with the specified name.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Access list configuration mode

Examples

The following example displays sample output of the **show ip access-lists** command.

```
device(config-ext-nacl)# show ip access-lists 111
Extended IP access list 111: 5 entries
bridged-routed
permit ip host 1.1.1.111 host 2.2.2.111
permit ospf any any
permit pim any any
deny ip 20.20.20.96 0.0.0.15 any
```

show ip client-pub-key

Displays the currently loaded public keys.

Syntax

show ip client-pub-key

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Examples

The following example displays sample output of the **show ip client-pub-key** command.

```
device(config)# show ip client-pub-key
---- BEGIN SSH2 PUBLIC KEY ----
Comment: DSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET W6ToHv8D1UJ/
z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH YI14Om
1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5cv
wHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9v
GfJ0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
```

show ipc_stats

Displays reliable IPC and dynamic queue statistics.

Syntax

show ipc_stats

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

NTP configuration mode

Examples

The following is a sample output of the **show ipc_stats** command.

```
device# show ipc_stats

Total available Hsync channel space = 1048580
Total available Appl channel space = 524292
Total number of application msgs in dyn queue = 0
Total number of hsync msgs in dyn queue = 0
Total number of rel sync msgs in dyn queue = 0
Total number of rx pkt msgs in standby dynamic queue = 0
Total number of rx pkt msgs in active dyn queue = 0
Total number of rx pkts relayed = 0
Total number of rx pkts received = 5686578
Total number of dyn-sync messages received so far = 3
Total number of rel-sync pending complete = 0
Total number of L3 baseline-sync packets = 655
Total number of packet drops in sync = 0
Is image_sync_in_progress? = 0
Total num of rx dyn queue drops = 0
Total num of jumbo corrupts = 0
Total number of messages in IP send queue = 0
```

show ip dhcp-server address-pool

Displays information about a specific DHCP address pool or all DHCP address pools.

Syntax

show ip dhcp-server address-pool [**pools**] [*name*]

Parameters

pools

Displays information about all the DHCP address pools.

name

Displays information about a specific address pool.

Modes

Global configuration mode

Command Output

The **show ip dhcp-server address-pool** command displays the following information:

Output field	Description
Pool name	The name of the address pool
Time elapsed since last save	The amount of time that has elapsed since the last save
Total number of active leases	The number of leases that are currently active
Address Pool State	The state of the address pool (active or inactive)
IP Address Exclusions	IP addresses that are not included in the address pool
bootfile	The name of the bootfile
dhcp-default-router	The address of the DHCP default router
dhcp-server-router	The address of the DHCP server router
dns-server	The address of the DNS server
domain-name	The name of the domain
lease	The identifier for the lease
ip-telephony-voice-server	The IP address of the voice server
ip-telephony-data-server	The IP address of the data server
wpad	The network location of the PAC file
xwindow manager	The IP addresses of systems that are running the X Window System Display Manager and are available to the client.
netbios-name-server	The address of the netBIOS name server
network	The address of the network
tftp-server	The IP address of the TFTP server
next-bootstrap-server	The IP address of the next-bootstrap server
vendor-class	The ASCII value of the DHCP client

Output field	Description
option	The value of the vendor specific information

Examples

The following example displays the IP DHCP server address pools.

```
device# show ip dhcp-server address-pools
Showing all address pool(s):
Pool Name: one
Time elapsed since last save: 0d:0h:6m:52s
Total number of active leases: 2
Address Pool State: active
IP Address Exclusions: 192.168.1.45
IP Address Exclusions: 192.168.1.99 192.168.1.103
Pool Configured Options:
bootfile: FI08030b_Manifest.txt
dhcp-default-router: 192.168.1.1
dns-server: 192.168.1.100
domain-name: example.com
lease: 0 0 30
ip-telephony-voice-server: MCIPADD=192.168.42.1,MCPORT=1719,TFTPSRVR=192.168.42.1
ip-telephony-data-server: MCIPADD=192.168.42.1,MCPORT=1719,TFTPSRVR=192.168.42.1
wpad: http://172.26.67.243:8080/wpad.dat
xwindow manager: 10.38.12.1 10.38.12.3 10.38.12.5
netbios-name-server: 192.168.1.101
network: 192.168.1.0 255.255.255.0
hostname: brocade_router
tftp-server:172.26.51.66
next-bootstrap-server: 192.168.1.102
vendor-class ascii:  "Ruckus CPE"
option: 43 hex 0108c0a80a01c0a81401
```

History

Release version	Command history
08.0.30b	This command was modified to include X Window System Display Manager updates in the output.
08.0.30mb	This command was modified to include the vendor class option in the output.
08.0.40	This command was modified to include updates in the output for WPAD, IP-telephony-voice, and data server.

show ip dhcp-server binding

Displays the IP DHCP server lease entry.

Syntax

show ip dhcp-server binding

Modes

Global configuration mode.

Usage Guidelines

The **show ip dhcp-server binding** command displays a specific DHCP active lease, or all active leases.

Command Output

The **show ip dhcp-server binding** command displays the following information:

Output field	Description
IP Address	The IP addresses currently in the binding database.
Client ID/Hardware address	The hardware address of the client.
Lease expiration	The time when this lease will expire.
Type	The type of lease.

Examples

The following example displays the IP DHCP server bindings.

```
device# show ip dhcp-server binding
Bindings from all pools:
IP Address Client-ID/ Lease expiration Type
Hardware address
192.168.1.2 0000.005d.a440 0d:0h:29m:31s Automatic
192.168.1.3 0000.00e1.26c0 0d:0h:29m:38s Automatic
```

show ip dhcp-server flash

Displays the lease-binding database stored in the flash memory.

Syntax

show ip dhcp-server flash

Modes

Global configuration mode

User EXEC mode

Command Output

The **show ip dhcp-server flash** command displays the following information:

Output field	Description
IP Address	The IP address of the flash memory lease-binding database.
Client-ID/Hardware address	The address of the client.
Lease expiration	The time when the lease will expire.
Type	The type of lease.

Examples

The following example displays details of the lease-binding database stored in the flash memory.

```
device# show ip dhcp-server flash
Address Pool Binding:
IP Address Client-ID/ Lease expiration Type
Hardware address
192.168.1.2 0000.005d.a440 0d:0h:18m:59s Automatic
192.168.1.3 0000.00e1.26c0 0d:0h:19m:8s Automatic
```

show ip dhcp-server summary

Displays the IP DHCP server summary.

Syntax

show ip dhcp-server summary

Modes

Global configuration mode.

User EXEC mode.

Usage Guidelines

The **show ip dhcp-server summary** command displays information about active leases, deployed address pools, undeployed address pools, and server uptime.

Command Output

The **show ip dhcp-server summary** command displays the following information:

Output field	Description
Total number of active leases	Indicates the number of leases that are currently active.
Total number of deployed address-pools	The number of address pools currently in use.
Total number of undeployed address-pools	The number of address pools being held in reserve.
Server uptime	The amount of time that the server has been active.

Examples

The following example displays the IP DHCP server summary.

```
device# show ip dhcp-server summary
DHCP Server Summary:
Total number of active leases: 2
Total number of deployed address-pools: 1
Total number of undeployed address-pools: 0
Server uptime: 0d:0h:8m:27s
```

show ip dhcp snooping flash

Displays the DHCP snooping learned entries from the flash file.

Syntax

show ip dhcp snooping flash

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show ip dhcp snooping flash** command displays the following information:

Output field	Description
DHCP snooping Info	Displays information about the saved DHCP entries in the flash file. This includes details about the total number of learned entries along with the IP address, MAC address, port number, VLAN, lease, and VRF name of each entry.

Examples

The following example displays the IP DHCP snooping flash information.

```
device# show ip dhcp snooping flash
Dhcp snooping Info
Total learnt entries 10
SAVED DHCP ENTRIES IN FLASH
   IP Address  Mac Address    Port          Virtual Port vlan  lease VRF
1  10.1.1.20   0000.0000.0001 1/1/1*2/1/25  v100         100   170   default-vrf
2  10.1.1.21   0000.0000.0002 1/1/1*2/1/25  v100         100   170   default-vrf
3  10.1.1.22   0000.0000.0003 1/1/1*2/1/25  v100         100   170   default-vrf
4  10.1.1.23   0000.0000.0004 1/1/1*2/1/25  v100         100   170   default-vrf
5  10.1.1.24   0000.0000.0005 1/1/1*2/1/25  v100         100   170   default-vrf
6  10.1.1.25   0000.0000.0006 1/1/1*2/1/25  v100         100   170   default-vrf
7  10.1.1.26   0000.0000.0007 1/1/1*2/1/25  v100         100   170   default-vrf
8  10.1.1.27   0000.0000.0008 1/1/1*2/1/25  v100         100   170   default-vrf
9  10.1.1.28   0000.0000.0009 1/1/1*2/1/25  v100         100   170   default-vrf
10 10.1.1.29   0000.0000.000a 1/1/1*2/1/25  v100         100   170   default-vrf
```

History

Release version	Command history
08.0.30b	This command was introduced.

show ip dhcp snooping info

Displays the DHCP snooping binding database.

Syntax

show ip dhcp snooping info

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

Beginning with FastIron release 08.0.30b, this command reads data from the DHCP binding database, and not from the flash file, as in releases prior to 08.0.30b.

Examples

The following example displays the DHCP snooping information.

```
device# show ip dhcp snooping info
Dhcp snooping Info
Total learnt entries 10
Learnt DHCP Snoop Entries
IP Address    Mac Address     Port           Virtual Port vlan  lease   VRF
10.1.1.20     0000.0000.0001 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.21     0000.0000.0002 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.22     0000.0000.0003 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.23     0000.0000.0004 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.24     0000.0000.0005 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.25     0000.0000.0006 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.26     0000.0000.0007 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.27     0000.0000.0008 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.28     0000.0000.0009 1/1/1*2/1/25    v100         100   200  default-vrf
10.1.1.29     0000.0000.000a 1/1/1*2/1/25    v100         100   200  default-vrf
```

The following example displays the DHCP snooping information on a switch image.

```
device(config-if-e1000-1/1/1)# show ip dhcp snoop info
Dhcp snooping Info
Total learnt entries 10
Learnt DHCP Snoop Entries
IP Address    Mac Address     Port           Virtual Port  vlan  lease VRF
10.1.1.20     0000.0000.0001 1/1/1*2/1/25    1/1/1*2/1/25   100   145   -
10.1.1.21     0000.0000.0002 1/1/1*2/1/25    1/1/1*2/1/25   100   145   -
10.1.1.22     0000.0000.0003 1/1/1*2/1/25    1/1/1*2/1/25   100   145   -
10.1.1.23     0000.0000.0004 1/1/1*2/1/25    1/1/1*2/1/25   100   145   -
10.1.1.24     0000.0000.0005 1/1/1*2/1/25    1/1/1*2/1/25   100   145   -
10.1.1.25     0000.0000.0006 1/1/1*2/1/25    1/1/1*2/1/25   100   145   -
10.1.1.26     0000.0000.0007 1/1/1*2/1/25    1/1/1*2/1/25   100   145   -
```

History

Release version	Command history
08.0.30b	This command was modified to include the output on a switch image.

show ip dhcp snooping vlan

Displays the DHCP snooping status for a VLAN and the trusted or untrusted ports.

Syntax

show ip dhcp snooping vlan *vlan-id*

Parameters

vlan-id

Specifies the VLAN ID.

Modes

Privileged EXEC mode

Command Output

The **show ip dhcp snooping vlan** command displays the following information:

Output field	Description
IP DHCP snooping VLAN #	Displays whether the IP DHCP snooping is enabled or disabled.

Examples

The following example displays the IP DHCP snooping status on VLAN 2.

```
device# show ip dhcp snooping vlan 2
IP DHCP snooping VLAN 2: Enabled
```

show ip interface ve

Displays the Internet Protocol (IP) interface Virtual Ethernet (VE) configurations.

Syntax

show ip interface ve *ve-num*

Parameters

ve-num

Specifies the VE interface number.

Modes

Global configuration mode

Privileged EXEC mode

User EXEC mode

Interface configuration mode

Usage Guidelines

The **show ip interface ve** command can be used to verify the VE down trigger delay time.

Examples

The following example displays the IP interface VE configurations.

```
device(config)# show ip interface ve 10

Interface Ve 10
    members: ethe 1/1/47 to 1/1/48 ethe 3/1/47
    active: ethe 1/1/47 to 1/1/48 ethe 3/1/47
    port enabled
    port state: UP
    ip address: 100.1.1.1         subnet mask: 255.255.255.0
    Port belongs to VRF: default-vrf
    encapsulation: ETHERNET, mtu: 1500, metric: 1
    directed-broadcast-forwarding: disabled
    ICMP redirect: enabled
    proxy-arp: disabled
    ip arp-age:  10 minutes
    delay notification timer: 20 seconds
    No Helper Addresses are configured.
    No inbound ip access-list is set
    No outgoing ip access-list is set
```

History

Release version	Command history
8.0.30b	This command was introduced.

show interfaces lag

Displays information about the LAG interface including counters.

Syntax

show interfaces lag [*lag-id* | *lag-name*]

Parameters

lag-id

Displays LAG information of a LAG specified by the LAG ID. If the specified LAG ID is not available, a warning message is displayed.

lag-name

Displays LAG information of a LAG specified by the LAG name. If the specified LAG name is not available, a warning message is displayed.

Modes

Privileged EXEC mode

Global configuration mode

Examples

The following command shows that the LAG specified by LAG ID 2 is not available in the system.

```
device(config)# show interfaces lag id2
Warning: can't find LAG id2
```

The following command shows LAG information of a lag1.

```
device(config)# show interfaces lag lag1
Total number of LAGs: 1
Total number of deployed LAGs: 1
Total number of trunks created:1 (127 available)
LACP System Priority / ID: 1 / 0000.0001.c000
LACP Long timeout: 90, default: 90
LACP Short timeout: 3, default: 3
=== LAG "lag1" ID 123 (static Deployed) ===
LAG Configuration:
Ports: e 1/1 to 1/2
Port Count: 2
Primary Port: 1/1
Trunk Type: hash-based
Deployment: Trunk ID 123, Active Primary none, base fid: 0x0800
Port Link Port-State Dupl Speed Trunk Tag Priori MAC Name Type
1/1 DisabNone None None 123 No level0 0000.0001.c000
default-port
1/2 DisabNone None None 123 No level0 0000.0001.c000
default-port
LAG lag1 Counters:
         InOctets        2237519128754          OutOctets      1050988054740
           InPkts           1968838581            OutPkts         2030408443
  InBroadcastPkts                    0   OutBroadcastPkts                   0
  InMulticastPkts                    0   OutMulticastPkts                   0
    InUnicastPkts           1968838581     OutUnicastPkts         2030448142
       InDiscards                    0        OutDiscards                   0
         InErrors                    0          OutErrors                   0
     InCollisions                    0      OutCollisions                   0
OutLateCollisions                    0
        Alignment                    0                FCS                   0
        GiantPkts                    0          ShortPkts                   0
     InBitsPerSec            782177316      OutBitsPerSec           466226351
     InPktsPerSec                90896      OutPktsPerSec               99992
    InUtilization                7.96%     OutUtilization                4.82%
```

The following command shows information about the LAG interface, including counters.

```
device(config)# show interfaces lag
Total number of LAGs:          1
Total number of deployed LAGs: 1
Total number of trunks created:1 (123 available)
LACP System Priority / ID:     1 / 748e.f8b1.66e0
LACP Long timeout:             120, default: 120
LACP Short timeout:            3, default: 3

=== LAG "test" ID 1 (dynamic Deployed) ===
LAG Configuration:
   Ports:         e 1/1/1 to 1/1/2
   Port Count:    2
   Primary Port:  1/1/1
   Trunk Type:    hash-based
   LACP Key:      20001
Deployment: HW Trunk ID 1
Port       Link    State   Dupl Speed Trunk Tag Pvid Pri MAC             Name
1/1/1      Up      Forward Full 1G    1     No  1    0   748e.f8b1.66e0
1/1/2      Up      Forward Full 1G    1     No  1    0   748e.f8b1.66e0
Port       [Sys P] [Port P] [ Key ] [Act][Tio][Agg][Syn][Col][Dis][Def][Exp][Ope]
1/1/1           1        1   20001   Yes   L   Agg  Syn  Col  Dis  No   No   Ope
1/1/2           1        1   20001   Yes   L   Agg  Syn  Col  Dis  No   No   Ope


 Partner Info and PDU Statistics
Port          Partner         Partner     LACP      LACP
            System MAC          Key     Rx Count  Tx Count
1/1/1       748e.f8b1.6020    20001       19        18
1/1/2       748e.f8b1.6020    20001       18        19
LAG test Counters:
        InOctets          91162279156          OutOctets           91155682034
           InPkts            171383016             OutPkts            171371929
  InBroadcastPkts             75449406    OutBroadcastPkts             75438497
  InMulticastPkts                10560    OutMulticastPkts                10553
    InUnicastPkts             95923050      OutUnicastPkts             95922879
        InBadPkts                    0
      InFragments                    0
       InDiscards                    0          OutErrors                    0
              CRC                    0         Collisions                    0
         InErrors                    0      LateCollisions                   0
      InGiantPkts                    0
      InShortPkts                    0
         InJabber                    0
   InFlowCtrlPkts                    0     OutFlowCtrlPkts                  0
     InBitsPerSec           1931301848       OutBitsPerSec           1931301848
     InPktsPerSec               453126       OutPktsPerSec               453126
    InUtilization              100.00%      OutUtilization              100.00%
```

History

Release version	Command history
08.0.30	This command was introduced.

show interfaces stack-ports

Use the **show interfaces stack-ports** command to display information about the stacking ports for all members in a stack.

Syntax

show interfaces stack-ports

Modes

Privileged EXEC mode

Usage Guidelines

Use the **clear stack ipc** command before issuing the**show stack ipc** command. This helps to ensure that the data are the most recent traffic statistics for the stack.

This command must be executed from active stack controller.

Command Output

The **show interfaces stack-ports** command displays the following information:

Output field	Description
Port	Specifies the stack identification number for this unit
Link	Identifies the configuration for modules on this unit
State	Indicates that a priority has been assigned to this stack unit
Dupl	Indicates whether the port is configured as half- or full-duplex
Speed	Indicates the port speed
Trunk	Indicates whether the port is part of a trunk
Tag	Indicates whether the port is tagged or untagged
P	Specifies port priority
MAC	Provides the MAC address of the port. **NOTE** If a unit is provisional (it is reserved and does not have a physical unit associated with the unit ID), the interface MAC address displayed for the unit is 0000.0000.0000.
Name	Displays the optional name assigned to the port if present

Examples

The following example displays information about the stack-port interfaces for an ICX 6610 in a mixed stack.

```
ICX6610-48 Router# show interfaces stack-ports
Port    Link    State   Dupl Speed Trunk Tag Pvid Pri MAC            Name
1/2/1   Up      Forward Full 40G   None  No  N/A  0   0000.0034.1db5
1/2/2   Up      Forward Full 10G   None  No  N/A  0   0000.0034.1db6
1/2/6   Up      Forward Full 40G   None  No  N/A  0   0000.0034.1db7
1/2/7   Down    None    None None  None  No  N/A  0   0000.0034.1db8
2/2/1   Down    None    None None  None  No  N/A  0   0000.0000.0000
2/2/2   Down    None    None None  None  No  N/A  0   0000.0000.0000
2/2/6   Down    None    None None  None  No  N/A  0   0000.0000.0000
2/2/7   Down    None    None None  None  No  N/A  0   0000.0000.0000
3/2/1   Down    None    None None  None  No  N/A  0   0000.0034.266d
3/2/2   Up      Forward Full 10G   None  No  N/A  0   0000.0034.266e
3/2/6   Up      Forward Full 40G   None  No  N/A  0   0000.0034.266f
3/2/7   Up      Forward Full 10G   None  No  N/A  0   0000.0034.2670
5/2/1   Down    None    None None  None  No  N/A  0   0000.0034.11ad
5/2/2   Up      Forward Full 10G   None  No  N/A  0   0000.0034.11ae
5/2/6   Up      Forward Full 40G   None  No  N/A  0   0000.0034.11af
5/2/7   Down    None    None None  None  No  N/A  0   0000.0034.11b0
```

show ip bgp neighbors

Displays configuration information and statistics for BGP4 neighbors of the device.

Syntax

show ip bgp neighbors

show ip bgp neighbors *ip-addr*

show ip bgp neighbors last-packet-with-error

show ipv6 bgp neighbors routes-summary

Parameters

ip-addr

IPv4 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

Privileged 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.

Examples

This example shows sample output from the show ip bgp neighbors command.

```
device# show ip bgp neighbors
  neighbors              Details on TCP and BGP neighbor connections
    Total number of BGP Neighbors: 1
1   IP Address: 192.168.1.1, AS: 7701000 (IBGP), RouterID: 192.168.1.1, VRF: default-vrf
    State: ESTABLISHED, Time: 0h3m33s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 49 seconds, HoldTimer Expire in 177 seconds
    Minimal Route Advertisement Interval: 0 seconds
       RefreshCapability: Received
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 1       0       5         0            0
       Received: 1       1       5         0            0
    Last Update Time: NLRI       Withdraw          NLRI       Withdraw
                  Tx: ---        ---           Rx: 0h3m33s    ---
    Last Connection Reset Reason:Unknown
    Notification Sent:     Unspecified
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer Negotiated IPV4  unicast  capability
      Peer configured for IPV4 unicast  Routes
    Neighbor AS4 Capability Negotiation:
      Peer Negotiated AS4  capability
      Peer configured for AS4  capability

 As-path attribute count: 1
    Outbound Policy Group:
       ID: 1, Use Count: 1
    TCP Connection state: ESTABLISHED, flags:00000044 (0,0)
     Maximum segment size: 1460
    TTL check: 0, value: 0, rcvd: 64
       Byte Sent:   148, Received: 203
       Local host:  192.168.1.2, Local  Port: 179
       Remote host: 192.168.1.1, Remote Port: 8041
       ISentSeq:    1656867  SendNext:    1657016  TotUnAck:          0
       TotSent:         149  ReTrans:          19  UnAckSeq:    1657016
       IRcvSeq:     1984547  RcvNext:     1984751  SendWnd:       64981
       TotalRcv:        204  DupliRcv:        313  RcvWnd:        65000
       SendQue:           0  RcvQue:            0  CngstWnd:       5840
```

show ip bgp summary

Displays summarized information about the status of all BGP connections.

Syntax

show ip bgp summary

Modes

User EXEC mode

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.

This field	Displays
State	The state of device sessions with each neighbor. The states are from this perspective of the device, not the neighbor. 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. • 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 the RoutesRcvd number. The difference indicates that this device filtered out some of the routes received in the UPDATE messages.

This field	Displays
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
```

show ip mroute

Displays information on multicast routes. You can specify whether you want to display information from static or connected mroutes or from a particular mroute.

Syntax

show ip mroute [**vrf** *vrf-name*] { **static** | **connected** | **nexthop** | *ip-subnet* [*mask*]}

Parameters

vrf *vrf-name*

Specifies a VRF route.

static

Specifies a static multicast route.

connected

Specifies a directly attached (connected) multicast route.

nexthop

Specifies an IPv4 next hop table.

ip-subnet [*mask*]

Specifies an IP address.

Modes

Privileged EXEC mode

Global configuration mode

Examples

The following example displays information for IP multicast routes:

```
Device(config)# show ip mroute

Total number of IP routes: 5
 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
        Destination             Gateway             Port            Cost         Type    Uptime
1       20.20.20.0/24           220.220.220.1       ve 220          1/1           S      8m54s
2       50.50.50.0/24           DIRECT              ve 50           0/0           D      8h26m
3       77.1.1.1/32             DIRECT              loopback 1      0/0           D      8h26m
4       129.129.129.0/24        DIRECT              ve 129          0/0           D      8h26m
5       220.220.220.0/24        DIRECT              ve 220          0/0           D      2h49m
```

The following example displays information for static multicast routes:

```
Device(config)# show ip mroute static

 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
        Destination             Gateway           Port           Cost    Type    Uptime
1       20.20.20.0/24           220.220.220.1     ve 220         1/1     S       8m54s
```

The following example displays information for directly attached multicast routes:

```
Device(config)# show ip mroute connected

 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
        Destination             Gateway          Port          Cost    Type    Uptime
1       50.50.50.0/24           DIRECT           ve 50         0/0     D       8h26m
2       77.1.1.1/32             DIRECT           loopback 1    0/0     D       8h26m
3       129.129.129.0/24        DIRECT           ve 129        0/0     D       8h26m
4       220.220.220.0/24        DIRECT           ve 220        0/0     D       2h49m
```

The following example displays information for IP multicast route 50.50.50.100:

```
Device(config)# show ip mroute 50.50.50.100

 Type Codes - B:BGP  D:Connected  S:Static;   Cost - Dist/Metric
        Destination             Gateway          Port          Cost    Type    Uptime
1       50.50.50.0/24           DIRECT           ve 50         0/0     D       8h26m
```

History

Release version	Command history
8.0.10a	This command was introduced.

show ip msdp mesh-group

Displays the details of a specific mesh-group.

Syntax

show ip msdp [**vrf** *vrf-name*] **mesh-group** *group-name*

Parameters

vrf

Displays the mesh-group details for the VRF instance specified by the *vrf-name* variable.

vrf-name

Specifies the VRF instance.

mesh-group

Specifies the MSDP group.

group-name

Specifies the mesh group.

Modes

Privileged EXEC mode

Global configuration mode

MSDP router configuration mode

Usage Guidelines

If used without specifying a VRF, this command shows data from the default VRF.

Command Output

The **show ip msdp** [**vrf** *vrf-name*] **mesh-group** *group-name* command displays the following information:

Output field	Description
Peer Address	The IP address of the MSDP peer that is placed in the mesh group.
State	The state of the MSDP device connection with the mesh group. The state can be one of the following: • CONNECT - The session is in the active open state. • ESTABLISH - The MSDP session is fully up. • IDLE - The session is idle. • LISTEN - The session is in the passive open state.
KA (Keep Alive) In	The number of MSDP keepalive messages received by the mesh group.
KA (Keep Alive) Out	The number of MSDP keepalive messages sent by the mesh group.
SA (Source-Active) In	The number of SA messages received by the mesh group.
SA (Source-Active) Out	The number of SA messages sent by the mesh group.

Output field	Description
NOT (Notification) In	The number of notification messages received by the mesh group.
NOT (Notification) out	The number of notification messages sent by the mesh group.
Age	The number of seconds the messages has been in the cache.

Examples

The following example shows the mesh-group configuration details.

```
device#show ip msdp mesh-group
Mesh-Group-Name                     Peer-IP-Address
group1                                40.0.0.40
group2                                21.0.0.23
```

The following example shows the details of mesh-group group1.

```
device#show ip msdp mesh-group group1
MSDP MESH-GROUP:group1
 KA: Keepalive SA:Source-Active NOT: Notification
 Peer Address    State          KA              SA             NOT         Age
                                In     Out     In     Out     In     Out
 40.0.0.40       ESTABLISH    1407    1406      0      0      0      0      6
```

The following example shows the mesh-group configuration details for the VRF 10 instance.

```
device#show ip msdp vrf 10 mesh-group
Mesh-Group-Name                     Peer-IP-Address
group1                                22.0.0.22
group2                                21.0.0.23
```

The following example shows the mesh-group group2 details for the VRF 10 instance.

```
device#show ip msdp vrf 10 mesh-group group2
MSDP MESH-GROUP:group2
KA: Keepalive SA:Source-Active NOT: Notification
Peer Address    State         KA           SA            NOT         Age
                                          In     Out    In     Out     In     Out
21.0.0.23           IDLE       0      0      0      0      0      0      0      0
```

History

Release version	Command history
08.0.20	This command was introduced.

show ip multicast group

Displays information about IGMP groups.

Syntax

show ip multicast [**cluster**] **group** [*group-address* [**detail**] [**tracking**]]

Parameters

cluster

Specifies a multi-chassis trunking (MCT) cluster.

group-address

Specifies information for a particular group.

detail

Specifies detailed IGMP group information for a specific group.

tracking

Specifies tracking information on interfaces that have tracking enabled.

Modes

Privileged EXEC mode

Command Output

The **show ip multicast group** command displays the following information:

Output Field	Description
group	The address of the group (destination address in this case, 224.1.1.1)
p-port	The physical port on which the group membership was received.
ST	**Yes** indicates that the IGMP group was configured as a static group; **No** means the address was learned from reports.
QR	**Yes** means the port is a querier port; No means it is not. A port becomes a non-querier port when it receives a query from a source with a lower source IP address than the device.
life	The number of seconds the group can remain in EXCLUDE mode. An EXCLUDE mode changes to INCLUDE mode if it does not receive an "IS_EX" or "TO_EX" message during a certain period of time. The default is 260 seconds. There is no life displayed in INCLUDE mode.
mode	Indicates current mode of the interface: INCLUDE or EXCLUDE. If the interface is in INCLUDE mode, it admits traffic only from the source list. If an interface is in EXCLUDE mode, it denies traffic from the source list and accepts the rest.
source	Identifies the source list that will be included or excluded on the interface. For example, if an IGMP V2 group is in EXCLUDE mode with a source of 0, the group excludes traffic from the 0 (zero) source list, which actually means that all traffic sources are included.

Examples

The following example shows that an IGMP V2 group is in EXCLUDE mode with a source of 0. The group excludes only traffic from the 0 (zero) source list, which means that all traffic sources are included.

```
Device#show ip multicast group
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 3 groups, 4 group-port, tracking_enabled
      group            p-port   ST     QR     life mode    source
1     224.1.1.2        1/33     no     yes    120  EX      0
2     224.1.1.1        1/33     no     yes    120  EX      0
3     226.1.1.1        1/35     yes    yes    100  EX      0
4     226.1.1.1        1/33     yes    yes    100  EX      0
```

The following example displays detailed IGMP group information for multicast group 226.1.1.1:

```
Device#show ip multicast group 226.1.1.1 detail
Display group 226.1.1.1 in all interfaces in details.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 1 groups, 2 group-port, tracking_enabled
      group            p-port   ST     QR     life mode    source
1     226.1.1.1        1/35     yes    yes    120  EX      0
    group: 226.1.1.1, EX, permit 0 (source, life):
      life=120, deny 0:
      group            p-port   ST     QR     life mode    source
2     226.1.1.1        1/33     yes    yes    120  EX      0
    group: 226.1.1.1, EX, permit 0 (source, life):
      life=120, deny 0:
```

The following example displays the list of clients that belong to multicast group 224.1.1.1 when tracking and fast leave are enabled:

```
Device#show ip multicast group 224.1.1.1 tracking
Display group 224.1.1.1 in all interfaces with tracking enabled.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 1 groups, 1 group-port, tracking_enabled
      group            p-port   ST     QR     life mode    source
*** Note: has 1 static groups to the entire vlan, not displayed here
1     224.1.1.1        1/33     no     yes    100  EX      0
    receive reports from 1 clients: (age)
      (10.2.100.2 60)
```

The following example displays information for a device in an MCT cluster, In the “local” column, YES indicates that report/leave were received on local ports [cluster-edge ports (CEP) or cluster-client-edge ports (CCEP)]; NO indicates that report/leave were received on a port that is an inter-chassis link (ICL) between the MCT cluster switches, via an MCT peer.

```
Device#show ip multicast cluster group
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 1 groups, 1 group-port
      group            p-port   ST     QR     life  mode    source     local
1     225.1.1.1        e3/10    no     no     260   EX      0          YES
2     230.1.1.2        e3/12    no     yes    40    EX      0          NO
```

History

Release version	Command history
8.0.20	This command was modified to display MCT cluster information.

show ip multicast mcache

Displays information in the multicast forwarding mcache.

Syntax

show ip multicast [**cluster**] **mcache**

Parameters

cluster

Specifies a multi-chassis trunking (MCT) cluster.

Modes

Privileged EXEC mode

Usage Guidelines

Configuring the **show default values** command does not show complete output; it shows only IGMP mcache values. The IGMP snooping mcache contains multicast forwarding information for VLANs and you must configure the **show ip multicast mcache** command to display those.

Command Output

The **show ip multicast mcache** command displays the following information:

Field	Description
(source group)	Source and group addresses of this data stream. (* group) means match group only; (source group) means match both.
cnt	The number of packets processed in software. Packets are switched in hardware, which increases this number slowly.
OIF	The output interfaces. If `entire vlan` is displayed, this indicates that static groups apply to the entire VLAN.
age	The mcache age. The mcache will be reset to 0 if traffic continues to arrive, otherwise the mcache will be aged out when it reaches the time defined by the **ip multicast mcache-age** command.
uptime	The up time of this mcache in seconds.
vidx	Vidx specifies output port list index. Range is from 4096 through 8191.
ref-cnt	The vidx is shared among mcaches having the same output interfaces. Ref-cnt indicates the number of mcaches using this vidx.
ICL	Inter-chassis link between MCT cluster switches.
CCEP	Cluster-client-edge ports (ports on cluster switch connecting it with acluster client).

Examples

The following example shows information in the multicast forwarding mcache:

```
Device#show ip multicast mcache
Example: (S G) cnt=: cnt is number of SW processed packets
    OIF: e1/22 TR(1/32,1/33), TR is trunk, e1/32 primary, e1/33 output
vlan 10, 1 caches. use 1 VIDX
1    (10.10.10.2 239.0.0.3) cnt=0
     OIF: tag e2
     age=2s up-time=2s change=2s vidx=8191 (ref-cnt=1)
```

The following example shows information in the multicast forwarding mcache when data arrives locally:

```
Device#show ip multicast cluster mcache
xample: (S G) cnt=: (S G) are the lowest 32 bits, cnt is number of SW processed packets
    OIF: e1/22 TR(e1/32,e1/33), TR is trunk, e1/32 primary, e1/33 output
         [1,10]: [1 - has local oif, 10 - ICL due to CCEP count]

vlan 10, 1 caches. use 1 VIDX
1    (* 225.1.1.3) cnt=52244
     OIF: tag TR(e4/23) [1,0]
     age=167s up-time=11548s, change=58639s vidx=8184 (ref-cnt=1)
```

The following example shows information in the multicast forwarding mcache when data arrives on an MCT peer:

```
Device#show ip multicast cluster mcache
Example: (S G) cnt=: (S G) are the lowest 32 bits, cnt is number of SW processed packets
    OIF: e1/22 TR(e1/32,e1/33), TR is trunk, e1/32 primary, e1/33 output
         [1,10]: [1 - has local oif, 10 - ICL due to CCEP count]

vlan 10, 1 caches. use 1 VIDX
1    (30.0.0.10 225.1.1.3) cnt=30084
     OIF: tag TR(e3/13) [1,0]
     age=152s up-time=13728s, change=9990s vidx=8184 (ref-cnt=1)
```

History

Release version	Command history
8.0.20	This command was modified to display MCT cluster information.

show ip multicast optimization

Displays Internet Group Management Protocol (IGMP) snooping hardware resource-sharing information.

Syntax

show ip multicast optimization [*ipmc-num*]

Parameters

ipmc-num

Specifies the IP multicast (IPMC) group index number.

Modes

Privileged EXEC mode

VLAN configuration mode

Usage Guidelines

The **show ip multicast optimization** command is available only on the ICX 7250, ICX 7450, and ICX 7750 devices.

Use this command to display the availability of IPMC group indexes in the hardware and how they are used and shared.

The IPMC group index range varies depending on the platform; values out of range are not displayed.

Examples

The following example displays resource information showing that IPMC group index 4 is shared by two users and the ports included in the set are 1/1/6 and 1/1/1:

```
Device(config)#vlan 150
Device(config-vlan-150)#show ip multicast optimization
Total IPMCs Allocated:    0; Available: 8192; Failed:    0
Index    IPMC         SetId         Users         Set
   1.    4             0x161fcbd8        2 {<1/1/6>,<1/1/1>,}
   2.    1             0x161d0930       10 {<1/1/6>,<1/1/4>,<1/1/3>,<1/1/2>,
                                           <1/1/1>,}
Sharability Coefficient:  76%
```

History

Release version	Command history
8.0.10	This command was introduced.

show ip multicast pimsm-snooping

Displays information related to PIM sparse mode (SM) snooping on the mcache.

Syntax

show ip multicast pimsm-snooping [**vlan** *vlan-id*] [**cache** *ip-address*] [**resources**]

Parameters

cache *ip-address*

Specifies the PIM SM Snooping cache.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **show ip multicast pimsm-snooping** command to display information related to the PIM SM snooping on the outgoing interface (OIF) in the mcache.

Examples

The following example shows PIM SM information for the mcache:

```
Device#show ip multicast pimsm-snooping
Example: Port: 7/3 (ref_count=1)
         ref_count: no of entries in pimsm snoop cache added this oif)

vlan 503, has 1 caches.
1    (* 225.1.1.1) has 3 pim join ports out of 4 OIF
     4/23 (ref_count=2), 4/13 (ref_count=1), 4/5 (ref_count=3),
```

show ip multicast vlan

Displays IGMP snooping information for a specific VLAN.

Syntax

show ip multicast vlan [**cluster**] *vlan-id*

Parameters

cluster

Specifies a Multi-Chassis Trunking (MCT) cluster.

vlan-id

Specifies the VLAN for which you want information. If you do not specify a *vlan-id*, information for all VLANs is displayed.

Modes

Privileged EXEC mode

Usage Guidelines

You can use the **show ip multicast vlan** command to display the querier information for a VLAN. This command displays the VLAN interface status and whether there is any other querier present with the lowest IP address. The following list provides the combinations of querier possibilities:

- Active Interface with no other querier present
- Passive Interface with no other querier present
- Active Interface with other querier present
- Passive Interface with other querier present

Command Output

The **show ip multicast vlan** command displays the following information:

Output Field	Description
Version	The global IGMP version.
Query	How often a querier sends a general query on the interface.
Group Age	The number of seconds membership groups can be members of this group before aging out.
Max Resp	The maximum number of seconds a client waits before replying to a query.
Other Qr	How long it took a switch with a lower IP address to become a new querier. This value is 2 x Query + Max Resp.
Unregistered IPv4 Multicast Packets Flooding	Indicates whether flooding is enabled.
cfg	The IGMP version for the specified VLAN.
vlan cfg	The IGMP configuration mode, which is either passive or active.
pimsm	Indicates that PIM SM is enabled on the VLAN.

Output Field	Description
rtr port	The router ports, which are the ports receiving queries.
local	Entries learned on local interfaces of the cluster switch, for example, the local client edge port (CCEP) or cluster edge port (CEP).
mct peer	Entries learned by way of the MCT peer cluster switch. Control messages synchronize by way of the inter-chassis link (ICL) from the MCT peer cluster switch.

Examples

The following example shows IGMP snooping information for VLAN 10:

```
Device#show ip multicast vlan 10
Version=3, Intervals: Query=10, Group Age=260, Max Resp=10, Other Qr=30
VL10: cfg V3, vlan cfg passive, , pimsm (vlan cfg), 3 grp, 1 (SG) cache, no rtr port,
  e2      has    3 groups, non-QR (passive), default V3
  **** Warning! has V2 client (life=240),
    group: 239.0.0.3, life = 240
    group: 224.1.1.2, life = 240
    group: 224.1.1.1, life = 240
  e4      has    0 groups, non-QR (passive), default V3
```

The following example shows IGMP snooping information when the VLAN interface is active and no other querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft
 V2, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port,
  1/1/16  has    0 groups,
This interface is Querier
default V2
  1/1/24  has    0 groups,
This interface is Querier
default V2
  2/1/16  has    0 groups,
This interface is Querier
default V2
  2/1/24  has    0 groups,
This interface is Querier
default V2
  3/1/1   has    0 groups,
This interface is Querier
default V2
  3/1/4   has    0 groups,
This interface is Querier
default V2
```

The following example shows IGMP snooping information when the VLAN interface is passive and no other querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft V2, vlan cfg passive, 0 grp, 0 (*G) cache, no rtr port,
  1/1/16  has    0 groups,
This interface is non-Querier (passive)
default V2
  1/1/24  has    0 groups,
This interface is non-Querier (passive)
default V2
  2/1/16  has    0 groups,
This interface is non-Querier (passive)
default V2
  2/1/24  has    0 groups,
This interface is non-Querier (passive)
default V2
  3/1/1   has    0 groups,
This interface is non-Querier (passive)
default V2
  3/1/4   has    0 groups,
This interface is non-Querier (passive)
default V2
```

The following example shows IGMP snooping information when the VLAN interface is active and another querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft V2, vlan cfg active, 7 grp, 6 (*G) cache, rtr ports,
    router ports: 2/1/24(260) 10.5.5.5, 3/1/4(260) 10.8.8.8,
  1/1/16  has    4 groups,
This interface is Querier
default V2
    group: 226.6.6.6, life = 240
    group: 228.8.8.8, life = 240
    group: 230.0.0.0, life = 240
    group: 224.4.4.4, life = 240
  1/1/24  has    1 groups,
This interface is Querier
default V2
    group: 228.8.8.8, life = 240
  2/1/16  has    4 groups,
This interface is Querier
default V2
    group: 226.6.6.6, life = 240
    group: 228.8.8.8, life = 240
    group: 230.0.0.0, life = 240
    group: 224.4.4.4, life = 240
  2/1/24  has    2 groups,
This interface is non-Querier
Querier is 10.5.5.5
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 234.4.4.4, life = 260
    group: 226.6.6.6, life = 260
  3/1/1   has    4 groups,
This interface is Querier
default V2
    group: 238.8.8.8, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  3/1/4   has    1 groups,
This interface is non-Querier
Querier is 10.8.8.8
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 236.6.6.6, life = 260
```

The following example shows IGMP snooping information when the VLAN interface is passive and another querier is present with the lowest IP address:

```
Device#show ip multicast vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=260
VL10: dft V2, vlan cfg passive, 7 grp, 6 (*G) cache, rtr ports,
    router ports: 2/1/24(260) 10.5.5.5, 3/1/4(260) 10.8.8.8,
  1/1/16  has    4 groups,
This interface is non-Querier (passive)
default V2
    group: 226.6.6.6, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  1/1/24  has    1 groups,
This interface is non-Querier (passive)
default V2
    group: 228.8.8.8, life = 260
  2/1/16  has    4 groups,
This interface is non-Querier (passive)
default V2
    group: 226.6.6.6, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  2/1/24  has    2 groups,
This interface is non-Querier (passive)
Querier is 10.5.5.5
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 234.4.4.4, life = 260
    group: 226.6.6.6, life = 260
  3/1/1   has    4 groups,
This interface is non-Querier (passive)
default V2
    group: 238.8.8.8, life = 260
    group: 228.8.8.8, life = 260
    group: 230.0.0.0, life = 260
    group: 224.4.4.4, life = 260
  3/1/4   has    1 groups,
This interface is non-Querier (passive)
Querier is 10.8.8.8
Age is 0
Max response time is 100
default V2
  **** Warning! has V3 (age=0)  nbrs
    group: 236.6.6.6, life = 260
```

The following example shows IGMP snooping information when the device is connected to an MCT cluster:

```
Device#show ip multicast cluster vlan 10
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255

VL10: dft V2, vlan cfg passive, 0 grp, 0 (*G) cache, rtr ports,
    router ports: e4/14(65) 50.0.0.1 (local:1, mct peer:0)

(local:1, mct peer:0)     <- Indicates if entry is local or\and mct-peer entry
```

The following example shows IGMP snooping information when flooding of unregistered IPv4 multicast frames is disabled:

```
Device#show ip multicast vlan
Summary of all vlans. Please use "sh ip mu vlan <vlan-id>" for details
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255

Unregistered IPv4 Multicast Packets Flooding: Disabled.

VL500: dft V2, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port,
VL600 no snoop: no global or local config
```

History

Release version	Command history
8.0.20	This command was modified to display MCT cluster information.
8.0.30	This command was modified to display flooding information.

show ip ospf interface

Displays information about all or specific OSPF-enabled interfaces.

Syntax

show ip ospf interface [*ip address*] [**brief**] [**ethernet** *mappedID/slot/port*] [**loopback** *number*] [**tunnel** *number*] [**ve** *vlan_id*]

Parameters

ip address
Specifies interface IP address in dotted decimal format.

brief
Displays brief summary information about the specified interface.

ethernet *mappedID/slot/port*
Specifies an Ethernet interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *number*
Specifies a loopback port number in the range of 1 to 255.

tunnel *number*
Specifies a tunnel interface.

ve *vlan_id*
Specifies the VLAN number.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **brief** keyword to limit the display to the following fields:

- Interface
- Area
- IP address
- Cost
- State
- Nbrs(F/C)

Command Output

The **show ip ospf interface** command displays the following information:

This field	Displays
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. • 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.
Interface bandwidth	The configured bandwidth on a tunnel interface for routing metric purposes only.
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

This field	Displays
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.
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.

Examples

This example shows sample output from the **show ip ospf interface** command when the **brief**keyword is used.

```
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    16.1.1.2/24   1     down  0/0
```

This example displays information about a specified OSPF-enabled VE interface.

```
device# show ip ospf interface ve 20

ve 20  admin up, oper up, ospf enabled, state up
     IP Address 21.21.21.22, Area 0
     Database Filter: Not Configured
     State BDR, Pri 1, Cost 1, Options 2, Type broadcast Events 31
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
     DR:  Router ID 3.3.3.3           Interface Address 21.21.21.21
     BDR: Router ID 2.2.2.2           Interface Address 21.21.21.22
                    Packets Received        Packets Sent
     Hello                      86374               86735
     Database                       2                   4
     LSA Req                        1                   0
     LSA Upd                      451                 907
     LSA Ack                      906                 451
     No Packet Errors!
     Neighbor Count = 1, Adjacent Neighbor Count= 1
     Neighbor:         21.21.21.21 [id 3.3.3.3] (DR)
     Authentication-Key: None
     MD5 Authentication: Key None, Key-Id None, Auth-change-wait-time 300
```

This example displays information about a specified OSPF-enabled Ethernet interface, including the cost, where the cost is calculated using the default interface speed and auto cost.

```
device# show ip ospf interface ethernet 3/1/1

     e 3/1/1 admin up, oper up, ospf enabled, state up
     IP Address 89.0.0.2, Area 0
     Database Filter: Not Configured
     State BDR, Pri 1, Cost 1, Options 2, Type broadcast Events 3
```

This example displays information about a specified OSPF-enabled Ethernet interface, including the cost, which has been calculated using the configured interface bandwidth and the default auto-cost.

```
device# show ip ospf interface ethernet 1/1/3

e 1/1/3 admin up, oper up, ospf enabled, state up
     IP Address 172.201.3.2, Area 0
     Database Filter: Not Configured
     State DR, Pri 1, Cost 34, Options 2, Type broadcast Events 5
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
     DR:  Router ID 192.168.3.1       Interface Address 172.201.3.2
     BDR: Router ID 192.168.1.1       Interface Address 172.201.3.1
                    Packets Received        Packets Sent
     Hello                          73                  79
     Database                        3                   2
     LSA Req                         0                   1
     LSA Upd                         4                   5
     LSA Ack                         5                   3
     No Packet Errors!
     Neighbor Count = 1, Adjacent Neighbor Count= 1
     Neighbor:         172.201.3.1 [id 192.168.1.1] (BDR)
     Authentication-Key: None
     MD5 Authentication: Key None, Key-Id None, Auth-change-wait-time 300
```

History

Release version	Command history
8.0.30	This command was modified to include configured bandwidth status.

show ip pim interface

Displays information for PIM interfaces.

Syntax

show ip pim interface { **ethernet** *stackid/slot/port-id* | **loopback** *loopback-number* | **ve** *ve-number* }

Parameters

ethernet *stackid/slot/port-id*

Specifies a physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *loopback-number*

Specifies a loopback interface.

ve *ve-number*

Specifies a virtual interface.

Modes

Privileged EXEC mode

Examples

This example displays output from the **show ip pim interface** command, showing that ACL 10 is applied to interface 1/1/9 to control neighbor access.

```
device# show ip pim interface
Flags    : SM  - Sparse Mode v2, DM - Dense Mode v2, P - Passive Mode

--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+

Int'face|Local          |Mode |St |Des Rtr|TTL|Mcast| Filter| VRF   |DR  |Override
        |Address        |     |   |AddPort|Thr|Bndry|  ACL  |       |Prio|Interval
--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+
e1/1/1   5.5.5.5         SM   Ena  Itself   1  None   None   default  1   3000ms
e1/1/9   15.1.1.5        SM   Ena  Itself   1  None   10     default  1   3000ms
e1/1/12  12.12.12.1      SM   Dis  Itself   1  None   None   default  1   3000ms
v20      21.21.21.22     SM   Ena  Itself   1  None   None   default  1   3000ms
v60      60.60.60.1      SM   Ena  Itself   1  None   None   default  1   3000ms
v310     110.110.110.2   SM   Dis  Itself   1  None   None   default  1   3000ms
v360     160.160.160.1   SM   Dis  Itself   1  None   None   default  1   3000ms
l2       4.4.4.4         SM   Ena  Itself   1  None   None   default  1   3000ms
l3       10.10.10.10     SM   Ena  Itself   1  None   None   default  1   3000ms
Total Number of Interfaces : 9
```

History

Release version	Command history
8.0.20a	This command was modified to display neighbor filter information.

show ip pim mcache

Displays the PIM multicast cache.

Syntax

show ip pim [**vrf** *vrf-name*] **mcache** [*source-address* | *group-address* | **counts** | **dense** | [**dit-idx** *dit-idx* | **g_entries** | **receiver** | **sg_entries** | **sparse** | **ssm**]

Parameters

vrf *vrf-name*
: Specifies information for a VRF instance.

source-address
: Specifies the multicast cache source address.

group-address
: Specifies the multicast cache group address.

counts
: Specifies the number of entries.

dense
: Specifies displaying only the PIM Dense Mode entries.

dit-idx *dit-idx*
: Specifies displaying all entries that match a specified downstream interface (DIT).

g_entries
: Specifies displaying only the (*, G) entries.

receiver
: Specifies displaying all entries that egress a specified interface.

sg_entries
: Specifies displaying only the (S, G) entries.

sparse
: Specifies displaying only the PIM Sparse Mode entries.

ssm
: Specifies displaying only the SSM entries.

Modes

Privileged EXEC mode

Command Output

The **show ip pim mcache** command displays the following information:

Output Field	Description
Total entries in mcache	The total number of PIM mcache entries
MJ	Membership Join
MI	Membership Include
ME	Membership Exclude - Legend for the mcache entry printed once per page, it gives the explanation of each of the flags used in the entry.
BR	Blocked RPT
BA	Blocked Assert
BF	Blocked Filter
BI	Blocked IIF
Uptime	Shows the entry uptime
upstream neighbor	Shows the upstream neighbor for the Source/RP based on the type of entry. For (*,G) it shows the upstream neighbor towards the RP. For (S,G) entries it shows the upstream neighbor towards the source.
Flags	Flags Represent Entry flags in hex format in the braces. And indicates the meaning of the flags set in abbreviated string whose explanations are as below. Only shows the flags which are set. SM - Shows If the entry is created by PIM Sparse Mode DM - Shows If DM mode entry is enabled SSM - Shows If the SSM mode entry is enabled RPT - Shows If the entry is on the rendezvous point (RP) SPT - Shows If the entry is on the source tree LSRC - Shows If the source is in a directly-connected interface LRcv - Shows If the receiver is directly connected to the router REG - if the data registration is in progress L2REG - if the source is directly connected to the router REGSUPP - if the register suppression timer is running RegProbe HW - Shows If the candidate for hardware forwarding is enabled FAST - Shows If the resources are allocated for hardware forwarding TAG - Shows If there is a need for allocating entries from the replication table MSDPADV - Shows If RP is responsible for the source and must be advertised to its peers. NEEDRTE - Shows If there is no route to the source and RP is available PRUNE - Shows If PIM DM Prune to upstream is required
RP	Shows the IP address of the RP.
fast ports	Shows forwarding port mask.
AgeSltMsk	Shows a value of 1 if the entry is programmed in hardware, and a value of 0 if it is not programmed in hardware.
L2 FID	Shows the hardware resource allocated for the traffic switched to receivers in the ingress VLAN.
DIT	Shows the hardware resource allocated for routed receivers.
RegPkt	Shows Count of Packets forwarded due to the Register decapsulation.

Output Field	Description
AvgRate	Shows the average Rate of packets ingressing for this entry over 30 seconds.
Profile	Shows the Profile ID associated with the Stream.
Number of matching entries	Shows the total number of mcache entries matching a particular multicast filter specified.
Outgoing interfaces Section	This section consists of three parts. L3 OIFs, L2OIFs and Blocked OIFs. And each section has Format of L3/L2/Blocked followed by (HW/SW) followed by count of the number of OIF in each section. Additionally, each section displays the OIFs one per line. And shows the OIF in the format eth/Tr(Vlan) followed by uptime/expiry time, followed by the Flags associated with each OIF.
L3	Shows whether the traffic is routed out of the interface.
L2	Shows whether the traffic is switched out of the interface.
HW	Shows whether the entry is hardware forwarded.
SW	Shows whether the entry is software forwarded
Eth/Tr(VL1)	Shows the outgoing interface on the specified VLAN.
Flags (explanation of flags in the OIF section)	Shows the flags set in each of the Outgoing interface in abbreviated string format whose explanations are as below. Legend of this shown at the top of each entry IM - Immediate IH - Inherited MJ - Membership Join MI - Membership Include ME - Membership Exclude BR - Blocked due to SG RPT BA - Blocked due to Assert BF - Blocked due to Filter BI - Blocked IIF (Incoming interface) matches OIF
Src-Vlan	Shows the VLAN associated with the ingress interface.
MCTPEERF - Traffic Forw By Cluster Peer CCEP	Applies only to Layer 3 multicast routing over MCT. This means multicast traffic for this stream is forwarded by cluster peer [remote] CCEP port because of flow load balancing

Examples

This example shows all PIM multicast cache entries:

```
Brocade(config)# show ip pim mcache
IP Multicast Mcache Table
Entry Flags : SM - Sparse Mode, SSM - Source Specific Multicast, DM - Dense Mode
       RPT - RPT Bit, SPT - SPT Bit, LSRC - Local Source, LRCV - Local Receiver
       HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For
        Replication Entry
       REGPROB - Register In Progress, REGSUPP - Register Suppression Timer
       MSDPADV - Advertise MSDP, NEEDRTE - Route Required for Src/RP, PRUN - DM
        Prune Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
       MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
       BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter, BI - Blocked IIF
Total entries in mcache: 20
1  (140.140.140.3, 225.0.0.1) in v340 (tag e8/1), Uptime 00:00:02
  Source is directly connected
  Flags (0x200004e1) DM HW FAST TAG
  fast ports: ethe 4/6 ethe 8/26
  AgeSltMsk: 1, L2 FID: 8188, DIT: 3 , AvgRate: 0, profile: none
  Forwarding_oif: 2
  L3 (HW) 2:
    TR(e4/6,e4/6)(VL330), 00:00:02/0, Flags: IM
    e8/26(VL310), 00:00:02/0, Flags: IM
  Src-Vlan: 340
```

This example shows the PIM multicast cache for the specified address:

```
Device(config)# show ip pim mcache 10.140.140.14 230.1.1.9
IP Multicast Mcache Table
Entry Flags : SM - Sparse Mode, SSM - Source Specific Multicast, DM - Dense Mode
     RPT - RPT Bit, SPT - SPT Bit, LSRC - Local Source, LRCV - Local Receiver
     HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For Replication Entry
     REGPROB - Register In Progress, REGSUPP - Register Suppression Timer
     MSDPADV - Advertise MSDP, NEEDRTE - Route Required for Src/RP, PRUN - DM Prune Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
     MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
     BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter, BI - Blocked IIF
Total entries in mcache: 20
1 (10.140.140.14, 230.1.1.9) in v1001 (tag e4/29), Uptime 00:03:12
  upstream neighbor 10.11.11.13
  Flags (0x600680e1) SM SPT LRCV HW FAST TAG
  fast ports: ethe 4/29 ethe 5/2
  AgeSltMsk: 1, L2 FID: 8188, DIT: 8 , AvgRate: 0, profile: none
  Forwarding_oif: 3, Immediate_oif: 0, Blocked_oif: 0
  L3 (HW) 2:
  e4/29(VL13), 00:03:12/0, Flags: MJ
  e5/2(VL1004), 00:03:12/0, Flags: MJ
  L2 (HW) 1:
  e5/2, 00:00:07/0, Flags: MJ
  L2 MASK: ethe 5/2
  Src-Vlan: 1001
```

This example shows the PIM multicast cache for the specified DIT:

```
Device#show ip pim mcache dit-idx 2
IP Multicast Mcache Table
Entry Flags    : SM  - Sparse Mode, SSM - Source Specific Multicast, DM - Dense Mode
                 RPT    - RPT Bit, SPT - SPT Bit, LSRC - Local Source, LRCV - Local Receiver
                 HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For Replication
Entry
                 REGPROB - Register In Progress, REGSUPP - Register Suppression Timer
                 MSDPADV - Advertise MSDP, NEEDRTE - Route Required for Src/RP,  PRUN - DM Prune
Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
                 MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
                 BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter, BI - Blocked IIF
Total entries in mcache: 30
1     (20.20.20.100, 225.1.1.1) in v220 (tag e1/1/13), Uptime 07:12:07
      upstream neighbor 220.220.220.1
      Flags (0x200680e1) SM SPT LRCV HW FAST TAG
      fast ports: ethe 1/1/11
      AgeSltMsk: 1,  L2 FID: 105c,  DIT:     2 , AvgRate: 0, profile: none
      Forwarding_oif: 1, Immediate_oif: 0, Blocked_oif: 0
      L3 (HW) 1:
          e1/1/11(VL40), 07:12:07/0, Flags: MJ
      Src-Vlan: 220
2     (20.20.20.100, 225.1.1.2) in v220 (tag e1/1/13), Uptime 00:01:00
      upstream neighbor 220.220.220.1
      Flags (0x200680e1) SM SPT LRCV HW FAST TAG
      fast ports: ethe 1/1/11
      AgeSltMsk: 1, L2 FID: 105c,  DIT:     2 , AvgRate: 0, profile: none
      Forwarding_oif: 1, Immediate_oif: 0, Blocked_oif: 0
      L3 (HW) 1:
          e1/1/11(VL40), 00:01:00/0, Flags: MJ
      Src-Vlan: 220
3     (20.20.20.100, 225.1.1.3) in v220 (tag e1/1/13), Uptime 00:01:00
      upstream neighbor 220.220.220.1
      Flags (0x200680e1) SM SPT LRCV HW FAST TAG
      fast ports: ethe 1/1/11
      AgeSltMsk: 1, L2 FID: 105c,  DIT:     2 , AvgRate: 0, profile: none
      Forwarding_oif: 1, Immediate_oif: 0, Blocked_oif: 0
      L3 (HW) 1:
          e1/1/11(VL40), 00:01:00/0, Flags: MJ
      Src-Vlan: 220
```

This example shows the PIM multicast cache with Layer 3 multicast routing over MCT, showing that multicast traffic for a stream is forwarded by a cluster peer CCEP port because of flow load balancing.

```
Device#show ip pim mcache
IP Multicast Mcache Table
Entry Flags    : SM  - Sparse Mode, SSM - Source Specific Multicast, DM - Dense Mode
                 RPT    - RPT Bit, SPT - SPT Bit, LSRC - Local Source, LRCV - Local Receiver
                 HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For Replication Entry
                 REGPROB - Register In Progress, REGSUPP - Register Suppression Timer
                 MSDPADV - Advertise MSDP, NEEDRTE - Route Required for Src/RP,  PRUN - DM Prune
Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert, MCTPEERF - Traffic Forw By Cluster
Peer CCEP
                 MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
                 BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter, BI - Blocked IIF
Total entries in mcache: 2

1     (39.39.39.1, 229.1.1.10) in v40 (tag e2/1/12), Uptime 00:21:31
      upstream neighbor 40.40.40.175
      Flags (0x200284e1) SM SPT HW FAST TAG
      fast ports: ethe 2/1/11
      AgeSltMsk: 1, IPMC:     4 , AvgRate: 0, profile: none
      Forwarding_oif: 1, Immediate_oif: 1, Blocked_oif: 0
      L3 (HW) 1:
          TR(e2/1/11,e2/1/11)(VL10), 00:21:31/178, Flags: IM  MCTPEERF
      Src-Vlan:   40
```

History

Release version	Command history
8.0.30h	The output of the command was modified to remove the rate counter.
8.0.40a	The output of the command was modified to remove the rate counter.
8.0.30	This command was modified to show output for Layer 3 multicast routing over MCT.

show ip pim neighbor

Displays information about PIM neighbors.

Syntax

show ip pim [**vrf** *vrf-name*] **neighbor** [**ethernet** *stack/slot/port* | **tunnel** *tunnel-id* | **ve** *ve-num*]

Parameters

vrf *vrf-name*

Displays information for the specified VRF instance.

ethernet *stack/slot/port*

Displays information for the specified Ethernet interface.

tunnel *tunnel-id*

Displays information for the specified Tunnel interface.

ve *ve-num*

Displays information for the specified VE interface.

Modes

User EXEC mode

Command Output

The **show ip pim neighbor** command displays the following information:

Output Field	Description
Port	The interface through which the device is connected to the neighbor.
Phyport	When there is a virtual interface, this is the physical port to which the neighbor is connected.
Neighbor	The IP interface of the PIM neighbor.
Holdtime sec	Indicates how many seconds the neighbor wants this device to hold the entry for this neighbor in memory. The neighbor sends the Hold Time in Hello packets: • If the device receives a new Hello packet before the Hold Time received in the previous packet expires, the device updates its table entry for the neighbor. • If the device does not receive a new Hello packet from the neighbor before the Hold time expires, the device assumes the neighbor is no longer available and removes the entry for the neighbor.
Age sec	The number of seconds since the device received the last hello message from the neighbor.
UpTime sec	The number of seconds the PIM neighbor has been up. This timer starts when the device receives the first Hello messages from the neighbor.

Output Field	Description
VRF	The VRF in which the interface is configured. This can be a VRF that the port was assigned to or the default VRF of the device.
Priority	The DR priority that is used in the DR election process. This can be a configured value or the default value of 1.

Examples

The following example shows information about PIM neighbors.

```
device(config)# show ip pim neighbor
--------+--------+---------------+--------+---+---------+---------+-----+-----------+-----------+----
Port    |PhyPort |Neighbor       |Holdtime|T  |PropDelay|Override |Age  |UpTime     |VRF        |Prio
        |        |               |sec     |Bit|msec     |msec     |sec  |           |           |
--------+--------+---------------+--------+---+---------+---------+-----+-----------+-----------+----
v2       e1/1/1     2.1.1.2         105      1   500       3000      0     00:44:10  default-vrf 1
v4       e1/2/2     4.1.1.2         105      1   500       3000      10    00:42:50  default-vrf 1
v5       e1/1/4     5.1.1.2         105      1   500       3000      0     00:44:00  default-vrf 1
v22      e1/1/1     22.1.1.1        105      1   500       3000      0     00:44:10  default-vrf 1
Total Number of Neighbors : 4
```

show ip pim traffic

Displays IPv4 PIM traffic statistics.

Syntax

show ip pim traffic [**vrf** *vrf-name*] [**join-prune**] [**rx** | **tx**]

Parameters

vrf *vrf-name*

Specifies information for a VRF instance.

join-prune

Specifies displaying join and prune statistics.

rx

Specifies displaying received PIM traffic statistics.

tx

Specifies displaying transmitted PIM traffic statistics.

Modes

Privileged EXEC mode

Usage Guidelines

PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

Command Output

The **show ip pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the PIM interface is configured.
HELLO	The number of PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface. **NOTE** Unlike PIM Dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface.

Output Field	Description
Err	The total number of messages discarded, including a separate counter for those that failed the checksum comparison.

Examples

This example shows PIM join and prune traffic statistics for received and sent packets:

```
device(config)# show ip pim traffic
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Rx        Rx          Rx        Rx        Rx        Rx        Rx        Rx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     0         0           0         0         0         0         0         0
v50     2526      1260        0         0         0         1263      0         0
v150    2531      0           0         0         0         1263      0         0
v200    2531      0           0         0         0         1         0         0
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     2528      0           0         0         0         0         0
v50     2540      1263        0         0         0         2         0
v150    2529      0           0         0         0         1262      0
v200    2529      0           0         0         0         1262      0
```

This example shows the number of received IPv4 PIM Hello packets dropped on interface 1/1/9 because an ACL to control neighbor access is configured on it.

```
device# show ip pim traffic rx
Port    HLO   JN-PRNE  ASSERT REG       REG       BTSTRP    CAND RP   Err
                              GRFT(DM)  STOP(SM)  MSGS(SM)  ADV.(SM)

-------+-------+------+-----+-------+----------+---------+---------+---
        Rx      Rx     Rx    Rx      Rx         Rx        Rx        Rx
-------+-------+------+-----+-------+----------+---------+---------+---
e1/1/1  0       0      0     0       0          0         0         0
e1/1/9  764     0      0     0       0          0         0         757
e1/1/12 0       0      0     0       0          0         0         0
v20     758     0      0     1916    0          0         0         0
v60     0       0      0     0       0          0         0         0
v310    0       0      0     0       0          0         0         0
v360    0       0      0     0       0          0         0         0
```

This example shows PIM join and prune traffic statistics for sent packets:

```
device(config)# show ip pim traffic tx
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     2528      0           0         0         0         0         0
v50     2540      1263        0         0         0         2         0
v150    2529      0           0         0         0         1262      0
v200    2530      0           0         0         0         1262      0
```

This example shows PIM join and prune traffic statistics.

```
device(config)# show ip pim traffic join-prune
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Rx        Rx        Rx        Rx        Rx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1260      1260      0         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Tx        Tx        Tx        Tx        Tx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1263      1262      1         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
```

This example shows PIM join and prune traffic statistics.

```
device(config)# show ip pim traffic join-prune rx
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Rx        Rx        Rx        Rx        Rx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1260      1260      0         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
```

This example shows PIM join and prune traffic statistics.

```
device(config)# show ip pim traffic join-prune tx
Port  Packet    Join      Prune     Avg Aggr  Last Aggr
-----+---------+---------+---------+---------+----------
      Tx        Tx        Tx        Tx        Tx
-----+---------+---------+---------+---------+----------
v30   0         0         0         0         0
v50   1264      1263      1         1         1
v150  0         0         0         0         0
v200  0         0         0         0         0
```

History

Release version	Command history
8.0.20a	This command was modified to display, in the Err column, received Hello packets dropped on an interface because of an ACL to control neighbor access.

show ip pimsm-snooping cache

Displays the downstream PIM join/prune information for both source-path tree (SPT) and rendezvous-point tree (RPT).

Syntax

show ip pimsm-snooping cache [**vlan** *vlan-id*] *ip-address* [**resources**]

Parameters

ip-address

Specifies the IP address.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **show ip pimsm-snooping cache** command to check and verify the outgoing interfaces (OIF)s added by pimsm-snooping module.

Command Output

The **show ip pimsm-snooping cache** command displays the following information:

Output field	Description
SG	(s,g) downstream fsm state for SPT.
G	(*,g) downstream fsm state for RPT

The **show ip pimsm-snooping cache** command displays the following information only when multi-chassis trunking (MCT) is enabled on the VLAN:

Output field	Description
CCEP	Cluster client edge port
CEP	Cluster edge port
Remote/Local	Join/Prune received on MCT peer or local

Examples

The following example shows PIM SM information when there is no traffic and the last-hop router (LHR) has joined the RPT. Only an (*,G) entry is created.

```
Device1#show ip pimsm-snooping cache
 OIF Info:
 TR - OIF Belongs to Trunk/LAG, Primary port is displayed
 SG - (*,g)/(s,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
 RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

PIMSM Snoop cache for vlan 503
1    (* 225.1.1.1) Up Time: 5d 18:38:32
    OIFs: 2
    TR(e4/5) G : J(197) ET: 210, Up Time: 5d 18:38:32 , CCEP, Remote
    TR(e4/23) G : J(166) ET: 210, Up Time: 1d 19:36:23 , CEP, Local
```

The following example shows PIM SM information when there is traffic from source 30.0.0.10. An (S,G) entry is created and the LHR has joined the SPT.

```
Device2#show ip pimsm-snooping cache
  OIF Info:
 TR - OIF Belongs to Trunk/LAG, Primary port is displayed
 SG - (*,g)/(s,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
 RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

1    (* 225.1.1.1) Up Time: 5d 18:44:28
    OIFs: 2
    TR(e4/5) G : J(195) ET: 210, Up Time: 5d 18:44:28 , CCEP, Remote
    TR(e4/23) G : J(170) ET: 210, Up Time: 1d 19:42:18 , CEP, Local

2    (30.0.0.10 225.1.1.1) Up Time: 00:00:58
    OIFs: 2
    TR(e4/5) SG : J(202) ET: 210, Up Time: 00:00:58 , CCEP, Remote
    TR(e4/23) SG : J(168) ET: 210, Up Time: 00:00:58 , CEP, Local
```

The following example shows PIM SM resource information.

```
Device#show ip pimsm-snooping resources
                     alloc in-use  avail get-fail    limit  get-mem  size init
pimsm group entry     1000     10    990        0   232000       10    61 1000
pimsm source entry    2000     20   1980        0   464000       40    65 2000
pimsm oif entry       2000     30   1970        0   464000       59    89 2000

Total memory in used: 369000 bytes
```

show ip reverse-path-check

Displays the global unicast Reverse Path Forwarding settings.

Syntax

show ip reverse-path-check

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show ip reverse-path-check** command displays the following information.

Output field	Description
CLI config	The command line configured on the device after device boot-up.
Current state	The mode set during device boot-up. This takes effect only after reload.

Examples

The following example shows the global uRPF settings on ICX 6610 devices.

```
device# show ip reverse-path-check
Global uRPF Settings:
CLI config : Strict mode
Current State : Strict mode
```

The following example shows the global uRPF settings on ICX 7750 devices.

```
device# show ip reverse-path-check
Global uRPF Settings:
CLI config : Enabled
Current State : Enabled
```

History

Release version	Command history
08.0.30	This command was introduced.

show ip reverse-path-check interface

Displays unicast Reverse Path Forwarding settings at the interface level on ICX 7750 devices.

Syntax

show ip reverse-path-check interface

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the interface level Unicast Reverse Path Forward settings such as the uRPF mode and whether uRPF is exclude default. Use the **show ip interface ethernet** command to view details about the interface level rpf-mode configuration.

Examples

The following example shows the interface level uRPF settings on ICX 7750 devices.

```
device# show ip reverse-path-check interface
------------------------------------------------------------------
 Interface           uRPF mode               uRPF Exclude default
------------------------------------------------------------------
 Eth 1/1/11          Strict                      No
```

History

Release version	Command history
08.0.30	This command was introduced.

show ip source-guard

Displays the learned IP addresses for IP Source Guard ports.

Syntax

show ip source-guard ethernet *stack-id/slot/port*

Parameters

ethernet*stack-id/slot/port*

Specifies the Ethernet interface.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show ip source-guard** command displays the following information:

Output field	Description
Interface	Displays the interface number for source guard entries learnt or configured statically.
Type	Displays the interface type - IP.
Filter mode	Displays the filter mode - active or inactive.
IP-address	The dynamically learned or statically configured address.
VLAN	Specifies the VLAN number.

Examples

The following output displays the learned IP addresses for IP Source Guard ports.

```
device# show ip source-guard e 1/1/48
Total IP Source Guard entries on port 1/1/48: 33
No     Interface           Type   Flter-mode      IP-address      Vlan
--     ---------           ----   ----------      ----------      ----
1      1/1/9*4/1/39         ip     active         15.15.15.127     1
2      1/1/9*4/1/39         ip     active         15.15.15.9       1
3      1/1/9*4/1/39         ip     active         15.15.15.10      1
4      1/1/9*4/1/39         ip     active         15.15.15.11      1
5      1/1/9*4/1/39         ip     active         15.15.15.12      1
6      1/1/9*4/1/39         ip     active         15.15.15.13      1
7      1/1/9*4/1/39         ip     active         15.15.15.14      1
8      1/1/9*4/1/39         ip     active         15.15.15.15      1
9      1/1/9*4/1/39         ip     active         15.15.15.16      1
10     1/1/9*4/1/39         ip     active         15.15.15.17      1
```

show ip ssh

Displays SSH connections details.

Syntax

show ip ssh [**config**]

Parameters

config

Displays the SSH configuration details.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show ip ssh** command displays the following information:

Output field	Description
Inbound	Connections listed under this heading are inbound.
Outbound	Connections listed under this heading are outbound.
Connection	The SSH connection ID.
Version	The SSH version number.
Encryption	The encryption method used for the connection.
Username	The username for the connection.
HMAC	The HMAC version.
Server Hostkey	The type of server host key. This can be DSA or RSA.
IP Address	The IP address of the SSH client.
SSH-v2.0 enabled	Indicates that SSHv2 is enabled.
hostkey	Indicates that at least one host key is on the device. It is followed by a list of the host key types and modulus sizes.

The **show ip ssh config** command displays the following information:

Output field	Description
SSH server	SSH server is enabled or disabled.
SSH port	SSH port number.

Output field	Description
Encryption	The encryption used for the SSH connection. The following values are displayed when AES only is enabled: • AES-256, AES-192, and AES-128 indicate the different AES methods used for encryption. • 3-DES indicates 3-DES algorithm is used for encryption
Permit empty password	Empty password login is allowed or not allowed.
Authentication methods	The authentication methods used for SSH. The authentication can have one or more of the following values: • Password - Indicates that you are prompted for a password when attempting to log into the device. • Public-key - Indicates that DSA or RSA challenge-response authentication is enabled. • Interactive - Indicates the interactive authentication is enabled.
Authentication retries	The number of authentication retries. This number can be from 1 through 5.
Login timeout (seconds)	SSH login timeout value in seconds. This can be from 0 through 120.
Idle timeout (minutes)	SSH idle timeout value in minutes. This can be from 0 through 240.
Strict management VRF	Strict management VRF is enabled or disabled.
SCP	SCP is enabled or disabled.
SSH IPv4 clients	The list of IPv4 addresses to which SSH access is allowed. The default is "All".
SSH IPv6 clients	The list of IPv6 addresses to which SSH access is allowed. The default is "All".
SSH IPv4 access-list	The IPv4 ACL used to permit or deny access using SSH.
SSH IPv6 access-list	The IPv6 ACL used to permit or deny access using SSH.

Examples

The following example displays sample output of the **show ip ssh** command.

```
device# show ip ssh
Connection  Version  Encryption  Username  HMAC       Server Hostkey  IP Address
Inbound:
1           SSH-2    3des-cbc    Raymond   hmac-sha1  ssh-dss         10.120.54.2
Outbound:
6           SSH-2    aes256-cbc  Steve     hmac-sha1  ssh-dss         10.37.77.15
SSH-v2.0 enabled; hostkey: DSA(1024), RSA(2048)
```

The following example displays sample output of the **show ip ssh config** command.

```
device# show ip ssh config
SSH server : Disabled
SSH port : tcp\22
Host Key :
Encryption : AES-256, AES-192, AES-128, 3-DES
Permit empty password : No
Authentication methods : Password, Public-key, Interactive
Authentication retries : 3
Login timeout (seconds) : 120
Idle timeout (minutes) : 0
SCP : Enabled
SSH IPv4 clients : All
SSH IPv6 clients : All
SSH IPv4 access-group :
SSH IPv6 access-group :
SSH Client Keys :
```

show ip ssl

Displays SSL connection details.

Syntax

show ip ssl certificate

Parameters

certificate

Displays the SSL certificate details.

Modes

Privileged EXEC mode

Global configuration mode

Examples

The following example displays the output of the **show ip ssl** command.

```
device(config)#show ip ssl
Session Protocol Source IP      Source Port  Remote IP      Remote Port
1       TLS_1_2  10.20.157.102  634          10.25.105.201  60892
```

The following example displays the SSL certificate details.

```
device(config)#show ip ssl certificate
Trusted Certificates:
 Dynamic:
 Index 0:
  Signature Algorithm: sha256WithRSAEncryption
  Issuer:
   CN: 10.25.105.201
  Validity:
   Not Before: 2014 Aug 22 05:12:45
   Not After : 2017 Aug 21 05:12:45
  Subject:
   CN: 10.25.105.201
  X509v3 extensions:
   X509v3 Subject Alternative Name:
    IP Address: 10.25.105.201
  Signature:
   12:ec:41:d8:01:45:61:ce:cf:7e:80:de:a6:7c:a7:2e:01:7f:
   42:27:22:1d:ac:a2:47:c5:0d:4f:e3:68:24:de:bf:50:40:65:
   25:8c:30:bd:ff:a7:d0:21:73:d2:ba:5e:67:42:1f:bb:97:4a:
   d9:1d:c3:ca:31:c4:59:10:79:d1:42:f4:b6:1a:b0:98:4e:a8:
   ef:e2:a2:98:c3:14:16:63:50:02:a0:18:9c:7a:e3:17:39:0d:
   b7:30:ab:23:9f:63:bd:0f:9e:d8:67:b0:fe:ec:3b:fa:4c:f4:
   3d:34:e2:99:0e:99:24:ec:93:fb:8a:e5:4a:bf:74:d6:ff:91:
   0a:dc:fb:b9:4f:91:5d:d4:f6:77:23:eb:ec:eb:3a:62:08:e1:
   a6:ea:a8:52:b6:39:62:db:29:fa:61:1d:fd:d5:02:31:04:73:
   50:ad:de:41:54:a5:e2:96:2d:9c:f4:68:b2:68:05:bb:39:47:
   ee:74:89:a2:8c:30:f0:f9:d7:d5:4b:3b:e2:95:6f:82:61:a3:
   c2:79:4c:f2:11:56:f8:2f:cc:fc:2b:4b:cb:3b:54:59:f0:8b:
   5b:70:e1:27:c3:57:25:eb:35:c6:07:ea:6d:0b:34:04:95:81:
   35:e6:64:c6:b8:72:e8:24:18:bd:ca:90:99:74:45:44:85:71:
   9e:7f:13:96:
```

show ip static-arp

Displays the static ARP entries along with static inspect ARP entries.

Syntax

show ip static-arp

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

The display index for static inspect ARP entries is not be displayed in the command output.

Command Output

The **show ip static-arp** command displays the following information:

Output field	Description
Static ARP table size	The maximum number of static ARP entries that can be configured. The default value is 512, and can be changed to 1024 using the **max-static-inspect-arp-entries** command.

Examples

The following example displays the static ARP.

```
device# show ip static-arp
Static ARP table size: 512, configurable from 512 to 1024
Index   IP Address          MAC Address       Port
1       207.95.6.111       0800.093b.d210     1/1/1
3       207.95.6.123       0800.093b.d211     1/1/1
-       1.1.1.1           0800.0000.0001     Invalid
```

History

Release version	Command history
08.0.30b	This command was modified. The output does not display the index for static inspect ARP entries.

show ip static mroute

Displays information for configured multicast routes.

Syntax

show ip static mroute [**vrf** *vrf-name*] *ip-subnet mask*]

Parameters

vrf *vrf-name*

Specifies an optional VRF route.

ip-subnet mask

Specifies an IP address and an optional address mask.

Modes

Privileged EXEC mode

Usage Guidelines

Only resolved and best static mroutes are added to the mRTM table. These routes are prefixed with an asterisk in the output from the **show ip static mroute** command.

Examples

The following example displays information for configured multicast routes:

```
Device(config)# show ip static mroute
IP Static Routing Table - 2 entries:
 IP Prefix          Next Hop        Interface  Dis/Metric/Tag  Name
*20.20.20.0/24      220.220.220.1   -          1/1/0
20.20.20.0/24       50.50.50.2      -          1/2/0
21.21.21.0/24       1.2.3.4         -          1/1/0
```

History

Release version	Command history
8.0.10a	This command was introduced.

show ipv6

Displays the IPv6 configuration details.

Syntax

show ipv6

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following is a sample output of the **show ipv6** command.

```
device# show ipv6
Global Settings
  IPv6 is enabled
  Link-local address(es):
    fe80::ce4e:24ff:fe8b:b050 [Preferred]
  Global unicast address(es):
  Joined group address(es):
    ff02::1:ff8b:b050
    ff02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 miliseconds
  ND retransmit interval is 1000 miliseconds
  Current Hop Limit is 64
  Hosts use stateless autoconfig for addresses
  No Inbound Access List Set
  No Outbound Access List Set
  No IPv6 Domain Name Set
  No IPv6 DNS Server Address set
```

show ipv6 access-list

Displays the IPv6 ACLs configured on a device.

Syntax

show ipv6 access-list [*acl-name*]

Parameters

acl-name

Specifies the IPv6 ACL name.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

ACL configuration mode

Examples

The following example displays information about all the IPV6 ACLs configured.

```
device# show ipv6 access-list
ipv6 access-list v6-ACL1: 1 entries
deny ipv6 any any
ipv6 access-list v6-ACL2: 1 entries
permit ipv6 any any
ipv6 access-list v6-ACL3: 2 entries
deny ipv6 2001:DB8:10::/64 any
permit ipv6 any any
ipv6 access-list v6-ACL4: 2 entries
deny ipv6 2001:DB8::/64 any
permit ipv6 any any
ipv6 access-list rate-ACL: 1 entries
permit ipv6 any any traffic-policy rate800M
ipv6 access-list v6-ACL5: 8 entries
permit tcp 2001:DB8::/64 any
permit ipv6 2001:DB8::/64 any
permit ipv6 2001:DB8:101::/64 any
permit ipv6 2001:DB8:10::/64 2001:DB8:102::/64
permit ipv6 host 2001:DB8:aa:10::102 host 2001:DB8:101::102
permit ipv6 host 2001:DB8:10::101 host 2001:DB8:101::101 dscp-matching 0
dscp-marking 63 dscp-cos-mapping
permit ipv6 any any dscp-matching 63 dscp-cos-mapping
permit ipv6 any any fragments
```

The following example displays information for a specific IPv6 ACL.

```
device# show ipv6 access-list rtr
ipv6 access-list rtr: 3 entries
remark This entry permits ipv6 packets from 2001:DB8::2 to any destination permit ipv6 host 2001:DB8::2
any
remark This entry denies udp packets from any source to any destination deny udp any any
remark This entry denies IPv6 packets from any source to any destination deny ipv6 any any
```

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

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 bgp neighbors** command.

```
device# show ipv6 bgp neighbors
    Total number of BGP Neighbors: 2
1   IP Address: 2001:1001::1, AS: 63753 (IBGP), RouterID: 1.0.0.1, VRF: default-vrf
       Description: SWD-2
    State: ESTABLISHED, Time: 0h47m50s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 26 seconds, HoldTimer Expire in 168 seconds
    Minimal Route Advertisement Interval: 0 seconds
       MD5 Password: $Qj0tZHMlXC1vbjYt
       UpdateSource: Loopback 1
       NextHopSelf: yes
       RefreshCapability: Received
       GracefulRestartCapability: Received
           Restart Time 120 sec, Restart bit 0
           afi/safi 2/1, Forwarding bit 0
       GracefulRestartCapability: Sent
           Restart Time 120 sec, Restart bit 0
           afi/safi 2/1, Forwarding bit 0
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
.....
```

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.

Output field	Description
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. **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

Output field	Description
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

  device# show ipv6 bgp summary
BGP4 Summary
 Router ID: 113.1.1.1   Local AS Number: 65020
 Confederation Identifier: not configured
 Confederation Peers:
 Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
 Number of Neighbors Configured: 2, UP: 1
 Number of Routes Installed: 5, Uses 430 bytes
 Number of Routes Advertising to All Neighbors: 7 (7 entries), Uses 336 bytes
 Number of Attribute Entries Installed: 4, Uses 360 bytes
 Neighbor Address     AS#   State  Time    Rt:Accepted Filtered Sent ToSend
 2001:db8:113:113::2  65001 CONN   1d14h32m       0      0     0      4
 2001:db8:400:400::2  65020 ESTAB  3h59m24s       2      0     3      0
```

show ipv6 dhcp-relay

Displays the DHCPv6 relay agent information configured on the device.

Syntax

show ipv6 dhcp-relay

Modes

Global configuration mode

Usage Guidelines

Command Output

The **show ipv6 dhcp-relay** command displays the following information:

Output field	Description
Current DHCPv6 relay agent state	Displays whether the current relay agent state is enabled or disabled.
DHCPv6 enabled interface(s)	Displays the DHCPv6 enabled interfaces.
DHCPv6 Relay Agent Statistics	Displays statistics such as the total number of DHCPv6 packets received and transmitted.
Received DHCPv6 Packets	The number of release, relay forward and relay reply packets received.

Examples

The following example displays the IPv6 DHCP relay statistics.

```
device(config)# show ipv6 dhcp-relay
Current DHCPv6 relay agent state: Enabled
DHCPv6 enabled interface(s): e 1/1/3
DHCPv6 Relay Agent Statistics:
Total DHCPv6 Packets, Received:0, Transmitted:0
Received DHCPv6 Packets: RELEASE:0,RELAY_FORWARD:0,RELAY_REPLY:0
OtherServertoClient:0,OtherClinettoServer:0
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

show ipv6 dhcp-relay delegated-prefixes

Displays information about the IPv6 delegated prefixes.

Syntax

show ipv6 dhcp-relay delegated-prefixes interface *interface-id*

Parameters

interface *interface-id*

Displays delegated prefixes for the specified outgoing interface.

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show ipv6 dhcp-relay delegated-prefixes** command displays the following information.

Output field	Description
IPv6 Prefix	The IPv6 prefix delegated to the client.
Client	The IPv6 address of the client.
Interface	The interface on which the DHCPv6 messages are relayed to the client.
ExpireTime	The remaining lifetime of the delegated prefix.

Examples

The following example displays information about the delegated prefixes.

```
device# show ipv6 dhcp-relay delegated-prefixes interface ethernet 1/1/45

Prefix                      Client              Interface  ExpireTime
fc00:2000:6:7:1::/96        fe80::210:94ff:fe00:e 1/1/45   29d23h53m0s
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

show ipv6 dhcp-relay destinations

Displays the IPv6 DHCP relay destinations.

Syntax

show ipv6 dhcp-relay destinations

Modes

Global configuration mode

Command Output

The **show ipv6 dhcp-relay destinations** command displays the following information:

Output field	Description
DHCPv6 Relay Destinations	The DHCPv6 relay agent configured destination information.

Examples

The following example displays the IPv6 DHCP relay destinations.

```
device# show ipv6 dhcp-relay destinations
DHCPv6 Relay Destinations:
Interface e 2/3:
Destination OutgoingInterface
2001::2 NA
fe80::224:38ff:febb:e3c0 e 2/5
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

show ipv6 dhcp-relay interface

Displays the IPv6 DHCP relay information for a specific interface.

Syntax

show ipv6 dhcp-relay interface

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.

Examples

The following example displays the DHCPv6 Relay information for an interface.

```
device# show ipv6 dhcp-relay interface ethernet 1/1/2
DHCPv6 Relay Information for interface e 1/1/2:
Destinations:
Destination OutgoingInterface
2001::2 NA
fe80::224:38ff:febb:e3c0 e 2/5
Options:
Interface-Id: Yes
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

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.

Examples

The following example displays relay options information.

```
device# show ipv6 dhcp-relay options
DHCPv6 Relay Options Information:
Interface    Interface-Id     Remote-Id
ve 100          No               No
ve 101          Yes              No
ve 102          No               Yes
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added.

show ipv6 dhcp-relay prefix-delegation-information

Displays information about the IPv6 DHCP prefix delegation.

Syntax

show ipv6 dhcp-relay prefix-delegation-information

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show ipv6 dhcp-relay prefix-delegation-information** command displays the following information:

Output field	Description
Interface	The interface name.
Current	The number of delegated prefixes currently learned on the interface.
Maximum	The maximum number of delegated prefixes that can be learned on the interface.
AdminDistance	The current administrative distance used for prefixes learned on this interface when added to the IPv6 static route table.

Examples

The following example displays information about the IPv6 DHCP delegated prefixes.

```
device# show ipv6 dhcp prefix-delegation-information
DHCPv6 Relay Prefix Delegation Notification Information:
Interface      Current    Maximum     AdminDistance
ve 100          20          20000         10
ve 101         4000         20000         10
ve 102           0          20000         10
ve 103           0          20000         10
ve 104           0          20000         10
ve 105           0          20000         10
```

History

Release version	Command history
08.0.10d	This command was introduced.
08.0.30	Support for this command was added in 08.0.30 and later releases.

show ipv6 dhcp6 snooping vlan

Displays the IPv6 DHCP snooping status on a VLAN.

Syntax

show ipv6 dhcp6 snooping vlan *vlan-name*

Parameters

vlan-name

The name of the VLAN.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example shows the status of DHCPv6 snooping enabled on VLAN 10.

```
device# show ipv6 dhcp6 snooping vlan 10
IP dhcpv6 snooping VLAN 10: Enabled
Trusted Ports: ethernet 1/1/1
Untrusted Ports: ethernet 1/1/2 ethernet 1/1/3
```

show ipv6 dhcp6 snooping info

Displays the DHCPv6 snooping binding database.

Syntax

show ipv6 dhcp6 snooping info

Modes

User EXEC mode

Usage Guidelines

Examples

The following example shows the DHCPv6 snooping learnt entries.

```
device# show ipv6 dhcp6 snooping info
IP dhcpv6 snooping enabled on 1 VLANS(s):
IPv6  Address  LinkLayer-Addr  Age  VRF
2002::24 0000.0343.0958 259198 0
2002::4a 7c00.030c.ccc9 259198 0
```

show ipv6 mroute

Displays information on IPv6 multicast routes. You can specify displaying information either from static or connected mroutes or from a particular mroute.

Syntax

show ipv6 mroute [**vrf** *vrf-name*] { *ipv6-address ipv6-prefix/prefix-length* | **static** | **connect** | **summary** }

Parameters

vrf *vrf-name*

Specifies displaying mroutes for a particular VRF.

ipv6-address ipv6-prefix/prefix-length

Displays an IPv6 mroute for the specified destination.

static

Displays only static multicast routes.

connect

Displays only connected multicast routes.

summary

Displays summary information.

Modes

Privileged EXEC mode

Examples

The following example displays information for IPv6 multicast routes:

```
Device(config)# show ipv6 mroute
IPv6 Routing Table - 7 entries:
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
S    1:1::1:0/120          ::                 ve 90         1/1            2d16h
C    2090::/64             ::                 ve 90         0/0            6d21h
C    2100::/64             ::                 ve 100        0/0            1d21h
C    2110::/64             ::                 ve 110        0/0            1d21h
C    2120::/64             ::                 ve 120        0/0            1d21h
C    2130::/64             ::                 ve 130        0/0            6d21h
C    8811::1/128           ::                 loopback 1    0/0            6d21h
```

The following example displays information for static IPv6 multicast routes:

```
Device(config)# show ipv6 mroute static
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
S    1:1::1:0/120          ::                 ve 90         1/1            2d16h
```

The following example displays information for directly attached (connected) IPv6 multicast routes:

```
Device(config)#show ipv6 mroute connect
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
C    2090::/64             ::                 ve 90         0/0            6d21h
C    2100::/64             ::                 ve 100        0/0            1d21h
C    2110::/64             ::                 ve 110        0/0            1d21h
C    2120::/64             ::                 ve 120        0/0            1d21h
C    2130::/64             ::                 ve 130        0/0            6d21h
C    8811::1/128           ::                 loopback 1    0/0            6d21h
```

The following example displays information for IPv6 multicast route 2090::1:

```
Device(config)# show ipv6 mroute 2090::1
Type Codes - B:BGP C:Connected S:Static
Type IPv6 Prefix           Next Hop Router    Interface     Dis/Metric     Uptime
C    2090::/64             ::                 ve 90         0/0            6d21h
```

History

Release version	Command history
8.0.10a	This command was introduced.

show ipv6 multicast mcache

Displays information in the IPv6 multicast forwarding mcache (multicast listening discovery [MLD]).

Syntax

show ipv6 multicast mcache

Modes

Privileged EXEC mode

Command Output

The **show ipv6 multicast mcache** command displays the following information:

Output Field	Description
(abcd:ef50 0:100):	The lowest 32 bits of source and group. It is displayed in XXXX:XXXX hex format. Here XXXX is a 16-bit hex number.
cnt	The number of packets processed in software.
OIF	Output interfaces.
age	The mcache age in seconds. The mcache is reset to 0 if traffic continues to arrive, otherwise it is aged out when it reaches the time defined by the **ipv6 multicast mcache-age** command.
uptime	The up time of this mcache in seconds.
vidx	The vidx is shared among mcaches using the same output interfaces. The vidx specifies the output port list, which shows the index. Valid range is from 4096 to 8191.
ref-cnt	The number of mcaches using this vidx.

Examples

This example shows information in the multicast forwarding mcache:

```
Device#show ipv6 multicast mcache
Example: (S G) cnt=: (S G) are the lowest 32 bits, cnt: SW proc. count
    OIF: 1/22 TR(1/32,1/33), TR is trunk, 1/32 primary, 1/33 output
vlan 1, has 2 cache
1    (abcd:ef50 0:100), cnt=121
     OIF: 1/11 1/9
     age=0s up-time=120s vidx=4130 (ref-cnt=1)
2    (abcd:ef50 0:101), cnt=0
     OIF: entire vlan
     age=0s up-time=0s vidx=8191 (ref-cnt=1)
vlan 70, has 0 cache
```

show ipv6 multicast group

Displays information about multicast listening discovery (MLD) groups.

Syntax

show ipv6 multicast group [*group-address* [**detail**] [**tracking**]]

Parameters

group-address

Specifies information for a particular group.

detail

Specifies the source list of a specific VLAN.

tracking

Specifies tracking information on interfaces that have tracking enabled.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 multicast group** command displays the following information:

Output Field	Description
group	The address of the IPv6 group (destination IPv6 address).
p-port	The physical port on which the group membership was received.
ST	**Yes** indicates that the MLD group was configured as a static group; **No** means it was learned from reports.
QR	**Yes** means the port is a querier port; **No** means it is not. A port becomes a non-querier port when it receives a query from a source with a lower source IP address than the port.
life	The number of seconds the group can remain in EXCLUDE mode. An EXCLUDE mode changes to INCLUDE if it does not receive an IS_EX or TO_EX message during a specified period of time. The default is 140 seconds. There is no `life` displayed in INCLUDE mode.
mode	The current mode of the interface: INCLUDE or EXCLUDE. If the interface is in INCLUDE mode, it admits traffic only from the source list. If the interface is in EXCLUDE mode, it denies traffic from the source list and accepts the rest.
source	Identifies the source list that will be included or excluded on the interface. An MLDv1 group is in EXCLUDE mode with a source of 0. The group excludes traffic from 0 (zero) source list, which actually means that all traffic sources are included.

Output Field	Description
group	If you requested a *detailed* report, the following information is displayed: • The multicast group address • The mode of the group • Sources from which traffic will be admitted (INCLUDE) or denied (EXCLUDE) on the interface. • The life of each source list. If you requested a *tracking/fast leave* report, the clients from which reports were received are identified.

Examples

This example shows that an MLDv1 group is in EXCLUDE mode with a source of 0. The group excludes only traffic from the 0 (zero) source list, which means that all traffic sources are included.

```
Device#show ipv6 multicast group
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 263 grp, 263 grp-port, tracking_enabled
      group                                 p-port ST QR life mode source
1     ff0e::ef00:a0e3                       1/7    N  Y  120  EX   0
2     ff01::1:f123:f567                     1/9    N  Y       IN   1
```

This example displays detailed MLD group information for multicast group ff0e::ef00:a096:

```
Device#show ipv6 multicast group ff0e::ef00:a096 detail
Display group ff0e::ef00:a096 in all interfaces in details.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 1 grp, 1 grp-port, tracking_enabled
      group                                 p-port ST QR life mode source
1     ff0e::ef00:a096                       1/7    N  Y  100  EX   0
    group: ff0e::ef00:a096, EX, permit 0 (source, life):
      life=100, deny 0:
```

This example displays the list of clients that belong to multicast group ff0e::ef00:a096 when tracking and fast leave are enabled:

```
Device#show ipv6 multicast group ff0e::ef00:a096 tracking
Display group ff0e::ef00:a096 in all interfaces with tracking enabled.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 1 grp, 1 grp-port, tracking_enabled
      group                                 p-port ST QR life mode source
1     ff0e::ef00:a096                       1/7    N  Y  80   EX   0
    receive reports from 1 clients: (age)
      (2001:DB8::1011:1213:1415 60)
```

show ipv6 multicast mcache

Displays information in the IPv6 multicast forwarding mcache (multicast listening discovery [MLD]).

Syntax

show ipv6 multicast mcache

Modes

Privileged EXEC mode

Command Output

The **show ipv6 multicast mcache** command displays the following information:

Output Field	Description
(abcd:ef50 0:100):	The lowest 32 bits of source and group. It is displayed in XXXX:XXXX hex format. Here XXXX is a 16-bit hex number.
cnt	The number of packets processed in software.
OIF	Output interfaces.
age	The mcache age in seconds. The mcache is reset to 0 if traffic continues to arrive, otherwise it is aged out when it reaches the time defined by the **ipv6 multicast mcache-age** command.
uptime	The up time of this mcache in seconds.
vidx	The vidx is shared among mcaches using the same output interfaces. The vidx specifies the output port list, which shows the index. Valid range is from 4096 to 8191.
ref-cnt	The number of mcaches using this vidx.

Examples

This example shows information in the multicast forwarding mcache:

```
Device#show ipv6 multicast mcache
Example: (S G) cnt=: (S G) are the lowest 32 bits, cnt: SW proc. count
    OIF: 1/22 TR(1/32,1/33), TR is trunk, 1/32 primary, 1/33 output
vlan 1, has 2 cache
1    (abcd:ef50 0:100), cnt=121
     OIF: 1/11 1/9
     age=0s up-time=120s vidx=4130 (ref-cnt=1)
2    (abcd:ef50 0:101), cnt=0
     OIF: entire vlan
     age=0s up-time=0s vidx=8191 (ref-cnt=1)
vlan 70, has 0 cache
```

show ipv6 multicast optimization

Displays multicast listening discovery (MLD) snooping hardware resource-sharing information.

Syntax

show ipv6 multicast optimization [*l2mc*]

Parameters

l2mc

Specifies the Layer 2 multicast (L2MC) group index.

Modes

Privileged EXEC mode

VLAN configuration mode

Usage Guidelines

The **show ipv6 multicast optimization** command is supported only on the ICX 7250, ICX 7450, and ICX 7750 devices.

Use this command to display the availability of L2MC group indexes in the hardware and how it is used and shared

The L2MC group index range varies depending on the platform. Values out of range are not displayed.

Examples

The following example displays resource information showing that L2MC group index 4 is shared by two users and the ports included in the set are 1/1/6 and 1/1/1:

```
Device (config)# vlan 150
Device (config-vlan-150)# show ipv6 multicast optimization
Total L2MCs Allocated:    0; Available: 8192; Failed:    0
Index    L2MC         SetId         Users         Set
   1.    4             0x161fcbd8        2 {<1/1/6>,<1/1/1>,}
   2.    1             0x161d0930       10 {<1/1/6>,<1/1/4>,<1/1/3>,<1/1/2>,
                                           <1/1/1>,}
Sharability Coefficient:  76%
```

History

Release version	Command history
8.0.10	This command was introduced.

show ipv6 multicast pimsm-snooping

Displays information related to PIM sparse mode (SM) snooping on the mcache.

Syntax

show ipv6 multicast pimsm-snooping [**vlan** *vlan-id*] [**cache** *ipv6-address*] [**resources**]

Parameters

cache *ipv6-address*

Specifies the PIM SM Snooping cache.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes

Privileged exec mode

Usage Guidelines

Use the **show ipv6 pimsm-snooping cache** command to display information related to the PIM SM snooping outgoing interface (OIF) in the mcache.

Examples

The following example shows PIM SM information for the mcache:

```
Device#show ipv6 multicast pimsm-snooping
Example: Port: 7/3 (ref_count=1)
         ref_count: no of entries in pimsm snoop cache added this oif)

vlan 503, has 1 caches.
1    (* 2:3) has 1 pim join ports out of 1 OIF
     1/1/4 (ref_count=2),
```

show ipv6 multicast vlan

Displays multicast listening discovery (MLD) snooping information for all VLANs or for a specific VLAN.

Syntax

show ipv6 multicast vlan *vlan-id*

Parameters

vlan-id

Specifies the VLAN for which you want information. If you do not specify a *vlan-id*, information for all VLANs is displayed.

Modes

Privileged EXEC mode

Command Output

The **show ipv6 multicast vlan** command displays the following information:

Output Field	Description
version	The MLD version number.
query-t	How often a querier sends a general query on the interface.
group-aging-t	Number of seconds membership groups can be members of this group before aging out.
rtr-port	The router ports which are the ports receiving queries. The display router ports: 1/36(120) 2001:DB8::2e0:52ff:fe00:9900 means port 1/36 has a querier with 2001:DB8::2e0:52ff:fe00:9900 as the link-local address, and the remaining life is 120 seconds.
max-resp-t	The maximum number of seconds a client can wait before it replies to the query.
non-QR	Indicates that the port is a non-querier.
QR	Indicates that the port is a querier.
Unregistered IPv6 Multicast Packets Flooding	Indicates whether flooding is enabled.

Examples

The following example shows MLD snooping information for VLAN 70:

```
Device#show ipv6 multicast vlan 70
version=1, query-t=60, group-aging-t=140, max-resp-t=3, other-qr-present-t=123
VL70: cfg V2, vlan cfg passive, 2 grp, 0 (SG) cache, rtr ports,
    router ports: 1/36(120) 2001:DB8::2e0:52ff:fe00:9900,
  1/26 has 2 grp, non-QR (passive), cfg V1
  1/26 has 2 grp, non-QR (passive), cfg V1
    group: ff10:1234::5679, life = 100
    group: ff10:1234::5678, life = 100
  1/35 has 0 grp, non-QR (QR=2001:DB8::2e0:52ff:fe00:9900, age=20), dft V2 trunk
```

The following example shows MLD snooping information when flooding of unregistered IPv6 multicast frames is disabled:

```
Device#show ipv6 multicast vlan
Summary of all vlans. use "sh ipv6 multicast vlan vlan-id" for details
Version=1, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255

Unregistered IPv6 Multicast Packets Flooding: Disabled.

VL500: dft V1, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port,
VL600 no snoop: no global or local config
```

History

Release version	Command history
8.0.30	This command was modified to display flooding information.

show ipv6 ospf interface

Displays interface information for all or specific OSPFv3-enabled interfaces.

Syntax

show ipv6 ospf interface [**brief**] [**ethernet** *mappedID/slot/port*] [**loopback** *number*] [**tunnel** *number*] [**ve** *vlan_id*]

Parameters

brief

Displays brief summary information about OSPFv3-enabled interfaces.

ethernet *mappedID/slot/port*

Specifies the physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *number*

Specifies a loopback port number in the range of 1 to 255.

tunnel *number*

Specifies a tunnel interface.

ve *vlan_id*

Specifies the VLAN number.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **brief** keyword to limit the display to the following fields:

- Interface
- Area
- Status
- Type
- Cost
- State
- Nbrs(F/C)

Command Output

The **show ipv6 ospf interface** command displays the following information:

This field	Displays
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.
Interface bandwidth	The configured bandwidth on a tunnel interface for routing metric purposes only.
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.
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.

This field	Displays
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.

Examples

This example shows sample output from the **show ipv6 ospf interface** command when no arguments or keywords are used.

```
device# show ipv6 ospf interface

e 1/1/9 admin up, oper up, IPv6 enabled
  IPv6 Address:
      fe80::224:10ff:fe76:4bc0
      201::1/64
  Instance ID 0, Router ID 2.2.2.2
  Area ID 0, Cost 1, Type BROADCAST
  MTU: 1500
  State DR, Transmit Delay 1 sec, Priority 1, Link-LSA Tx not suppressed
  Timer intervals :
    Hello 10, Hello Jitter 10  Dead 40, Retransmit 5
  Authentication Use: Enabled
   KeyRolloverTime(sec): Configured: 300 Current: 0
   KeyRolloverState: NotActive
   Outbound: None
   Inbound: None
  DR:2.2.2.2 BDR:1.1.1.1  Number of I/F scoped LSAs is 2
  DRElection:     2 times, DelayedLSAck:   425 times
  Neighbor Count = 1,   Adjacent Neighbor Count= 1
     Neighbor:
      1.1.1.1 (BDR)
    Statistics of interface e 1/1/9:
      Type     tx         rx         tx-byte    rx-byte
      Unknown  0          0          0          0
      Hello    80035      80133      3201392    3205320
      DbDesc   5          3          240        144
      LSReq    1          1          28         76
      LSUpdate 2095       1262       171228     92540
      LSAck    425        419        32020      48604
      OSPF messages dropped,no authentication: 0
```

This example shows sample output from the **show ipv6 ospf interface** command when the **brief** keyword is used.

```
device# show ipv6 ospf interface brief
Interface     Area        Status Type Cost  State    Nbrs(F/C)
e 1/1/9       0           up     BCST 1     DR       1/1
e 1/1/12      0           down   BCST 0     Down     0/0
ve 20         0           up     BCST 1     DR       0/0
ve 60         0           up     BCST 1     DR       0/0
ve 310        0           down   BCST 0     Down     0/0
ve 360        0           down   BCST 0     Down     0/0
loopback 1    0           up     BCST 1     Loopback 0/0
loopback 2    0           up     BCST 1     Loopback 0/0
loopback 3    0           up     BCST 1     Loopback 0/0
```

This example shows information about a specified OSPF-enabled Ethernet interface, including the cost, where the cost is calculated using the default interface speed and auto cost.

```
device# show ipv6 ospf interface ethernet 3/1/1

     e 3/1/1 admin up, oper up, ospf enabled, state up
     fe80::224:10ff:fe76:4bc0
      201::1/64,
     Area 0
     Database Filter: Not Configured
     State BDR, Pri 1, Cost 1, Options 2, Type broadcast Events 3
```

This example shows information about a specified OSPF-enabled Ethernet interface, including the cost, which has been calculated using the configured interface bandwidth and the default auto-cost.

```
device# show ipv6 ospf interface ethernet 3/1/1

     e 1/1/3 admin up, oper up, IPv6 enabled
  IPv6 Address:
      fe80::ce4e:24ff:fe6d:bc00
      9000:1111:9013::2/64
  Instance ID 0, Router ID 192.168.3.1
  Area ID 0, Cost 34, Type BROADCAST
  MTU: 1500
  State DR, Transmit Delay 1 sec, Priority 1, Link-LSA Tx not suppressed
  Timer intervals :
    Hello 10, Hello Jitter 10  Dead 40, Retransmit 5
  Authentication Use: Enabled
   KeyRolloverTime(sec): Configured: 300 Current: 0
   KeyRolloverState: Not Active
   Outbound: None
   Inbound: None
  DR:192.168.3.1 BDR:192.168.1.1  Number of I/F scoped LSAs is 2
  DRElection:     2 times, DelayedLSAck:     1 times
  Neighbor Count = 1,   Adjacent Neighbor Count= 1
     Neighbor:
      192.168.1.1 (BDR)
    Statistics of interface e 1/1/3:
      Type     tx         rx         tx-byte    rx-byte
      Unknown  0          0          0          0
      Hello    82         78         3268       3120
      DbDesc   2          3          116        304
      LSReq    1          1          148        28
      LSUpdate 16         7          1144       1048
      LSAck    1          3          156        328
      OSPF messages dropped, no authentication: 0
```

History

Release version	Command history
8.0.30	This command was modified to include configured bandwidth status.

show ipv6 neighbor

Displays the status of the neighbor discovery (ND) inspection configuration, details of the VLANs on which ND inspection is enabled, ND static entries, and ND inspection statistics.

Syntax

show ipv6 neighbor [**vrf** *vrf-name*] **inspection** [**static-entry** | **statistics** | **vlan** *vlan-number*]

Parameters

static-entry
Specifies the manually configured static ND inspection entries that are used to validate the packets received on untrusted ports.

statistics
Specifies the total number of neighbor discovery messages received and the number of packets discarded after ND inspection.

vlan
Specifies the VLANs on which ND inspection is enabled.

vlan-number
Specifies the ID of the configured VLAN.

vrf
Specifies the VRF instance.

vrf-name
Specifies the ID of the VRF instance.

inspection
Specifies that the neighbor discovery messages are verified against the static ND inspection entries or dynamically learned DHCPv6 snoop entries.

Modes

Privileged EXEC mode

Global configuration mode

VRF configuration mode

Command Output

The **show ipv6 neighbor** command displays the following information.

Output field	Description
VLAN	The list of VLANs on which ND inspection is enabled.
IPv6 Address	The IPv6 addresses of the hosts that are added as static ND inspection entries.
LinkLayer-Addr	The MAC addresses of the hosts that are added as static ND inspection entries.
Total number of ND Solicit received	The total number of neighbor solicitation messages received.
Total number of ND Advert received	The total number of neighbor advertisement messages received.

Output field	Description
Total number of Router Solicit received	The total number of router solicitation messages received.
Total number of ND dropped	The total number of neighbor discovery messages that are discarded because of the IP-to-MAC address binding discrepancy.
IPv6 Neighbor inspection VLAN *vlan-number*	The status of ND inspection on a VLAN.
Untrusted Ports	The interfaces or member ports on which trust mode is not enabled.
Trusted Ports	The interfaces or member ports on which trust mode is enabled.

Examples

The following example shows the output of the **show ipv6 neighbor inspection** command.

```
device(config)# show ipv6 neighbor inspection
IPv6 Neighbor inspection enabled on 2 VLAN(s):
        VLAN: 2
        VLAN: 3
```

The following example shows the output of the ND inspection configuration details for a VRF.

```
device(config-vrf-3)# show ipv6 neighbor vrf 3 inspection
IPv6 Neighbor inspection enabled on 2 VLAN(s):
        VLAN: 2
        VLAN: 3
```

The following example shows the output of the **show ipv6 neighbor inspection static-entry** command.

```
device(config)# show ipv6 neighbor inspection static-entry
 Total number of ND Inspect entries: 3
 IPv6 Address                           LinkLayer-Addr
 2001::1                                0000.0000.1234
 2001::3                                0000.1234.4567
 2001::2                                0000.0000.4567
```

The following example shows the ND static entries of a VRF.

```
device(config-vrf-3)# show ipv6 neighbor vrf 3 inspection static-entry
 Total number of ND Inspect entries: 1
 IPv6 Address                           LinkLayer-Addr
 2001:201:1:1::34                        cc4e.246d.2038
```

The following example shows the output of the **show ipv6 neighbor inspection statistics** command.

```
device(config)# show ipv6 neighbor inspection statistics
Total number of ND Solicit received      11
Total number of ND Advert received      29
Total number of Router Solicit received  20
Total number of ND dropped               6
```

The following example shows the ND inspection statistics of a VRF.

```
device(config-vrf-3)# show ipv6 neighbor vrf 3 inspection statistics
Total number of ND Solicit received      11
Total number of ND Advert received      29
Total number of Router Solicit received  20
Total number of ND dropped               6
```

The following example shows the output of the **show ipv6 neighbor inspection vlan** *vlan-number* command.

```
device (config)# show ipv6 neighbor inspection vlan 2
IPv6 Neighbor inspection VLAN 2: Enabled
  Untrusted Ports : ethe 1/1/1 to 1/1/2
  Trusted Ports : ethe 1/1/3
```

The following example shows the details of the VLANs on which ND inspection is enabled for a VRF.

```
device (config-vrf-3)# show ipv6 neighbor vrf 3 inspection vlan 2
IPv6 Neighbor inspection VLAN 2: Enabled
  Untrusted Ports : ethe 1/1/1 to 1/1/2
  Trusted Ports : ethe 1/1/3
```

History

Release version	Command history
08.0.20	This command was introduced.

show ipv6 pim interface

Displays information for IPv6 PIM interfaces.

Syntax

show ipv6 pim interface { **ethernet***stackid/slot/port-id* | **loopback** *loopback-number* | **ve** *ve-number* }

Parameters

ethernet*stackid/slot/port-id*

Specifies a physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

loopback *loopback-number*

Specifies a loopback interface.

ve *ve-number*

Specifies a virtual interface.

Modes

Privileged EXEC mode

Examples

The following example displays output from the **show ipv6 pim interface** command, showing that ACL f10 is applied to interface 1/1/9 to control neighbor access.

```
Device# show ipv6 pim interface
Flags     : SM  - Sparse Mode v2

--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+

Int'face|Local          |Mode |St |Des Rtr|TTL|Mcast| Filter| VRF   |DR  |Override
        |Address        |     |   |Add Prt|Thr|Bndry|  ACL  |       |Prio|Interval
--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+
e1/1/1   3000::2         SM   Ena  Itself   1  None   None   default  1   3000ms
e1/1/9   201::1          SM   Ena  Itself   1  None   f10    default  1   3000ms
e1/1/12  1222::1         SM   Dis  Itself   1  None   None   default  1   3000ms
v20      2000::2         SM   Ena  Itself   1  None   None   default  1   3000ms
v60      6000::1         SM   Ena  Itself   1  None   None   default  1   3000ms
v310     1100::2         SM   Dis  Itself   1  None   None   default  1   3000ms
v360     1600::1         SM   Dis  Itself   1  None   None   default  1   3000ms
l2       4444::2         SM   Ena  Itself   1  None   None   default  1   3000ms
l3       7711::11        SM   Ena  Itself   1  None   None   default  1   3000ms
Total Number of Interfaces : 9
```

History

Release version	Command history
8.0.20a	This command was modified to display neighbor filter information.

show ipv6 pim traffic

Displays IPv6 PIM traffic statistics.

Syntax

show ipv6 pim traffic [**vrf** *vrf-name*] [**join-prune**] [**rx** | **tx**]

Parameters

vrf *vrf-name*

Specifies information for a VRF instance.

join-prune

Specifies displaying join and prune statistics.

rx

Specifies displaying received PIM traffic statistics.

tx

Specifies displaying transmitted PIM traffic statistics.

Modes

Privileged EXEC mode

Usage Guidelines

PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

Command Output

The **show ipv6 pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the IPv6 PIM interface is configured.
HELLO	The number of IPv6 PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface. **NOTE** Unlike PIM dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.

Output Field	Description
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface. Register Graft (DM)
Err	The total number of MLD messages discarded, including a separate counter for those that failed the checksum comparison.

Examples

This example shows PIM traffic statistics:

```
Device# show ipv6 pim traffic
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS  (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Rx        Rx          Rx        Rx        Rx        Rx        Rx        Rx
------+---------+-----------+---------+---------+---------+---------+---------+---
v170    0         0           0         0         0         0         0         0
v501    0         0           0         0         0         0         0         0
v503    3302      2524        0         0         0         0         0         0
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS  (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v170    3576      0           0         0         0         0         0
v501    1456      0           0         0         0         0         0
v503    1456      1314        0         0         0         2         0
```

This example shows the number of received IPv6 PIM Hello packets dropped on interface 1/1/9 to because an ACL to control neighbor access is configured on it.

```
Device#show ipv6 pim traffic rx
Port    HELLO  JN-PRN  ASSERT  REG      REG       BTSTRP     CAND RP  Err
                               GRFT(DM) STOP(SM)  MSGS(SM)   ADV.(SM)

-------+------+------+------+------+---------+----------+-----
        Rx       Rx      Rx     Rx     Rx        Rx        Rx
Rx
-------+-------+------+------+------+------+---------+---------+------
e1/1/1  0       0        0      0      0         0         0      0
e1/1/9  924     0        0      0      0         5         0      914
e1/1/12 0       0        0      0      0         0         0      0
v20     0       0        0      0      0         0         0      0
v60     0       0        0      0      0         0         0      0
v310    0       0        0      0      0         0         0      0
v360    0       0        0      0      0         0         0      0
```

History

Release version	Command history
8.0.20a	This command was modified to display, in the Err column, received Hello packets dropped on an interface because of an ACL to control neighbor access.

show ipv6 pimsm-snooping cache

Displays the downstream PIM join/prune information for both source-path tree (SPT) and rendezvous-point tree (RPT).

Syntax

show ipv6 pimsm-snooping cache [**vlan** *vlan-id*] *ipv6-address* [**resources**]

Parameters

ipv6-address

Specifies the IP address.

vlan *vlan-id*

Specifies snooping for a VLAN.

resources

Specifies PIM SM snooping resources.

Modes

Privileged exec mode

Command Output

The **show ipv6 pimsm-snooping cache** command displays the following information:

Output field	Description
SG	(s,g) downstream fsm state for SPT.
G	(*,g) downstream fsm state for RPT

The **show ipv6 pimsm-snooping cache** command displays the following information only when multi-chassis trunking (MCT) is enabled on the VLAN:

Output field	Description
CCEP	Cluster-client-edge port
CEP	Cluster-edge port
Remote/Local	Join/Prune received on MCT peer or local

Examples

The following example shows PIM SM information.

```
Device#show ipv6 pimsm-snooping cache
 OIF Info:
TR - OIF Belongs to Trunk/LAG, Primary port is displayed
SG - (s,g) downstream fsm state:
G - (*,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

PIMSM Snoop cache for vlan 503
1    (* ff7e::1:2:3) Up Time: 03:43:40
                OIF: 1
                TR(e1/1/4) G : J(183) ET: 210, Up Time: 03:43:40

2    (3000::10 ff7e::1:2:3) Up Time: 00:02:52
                OIF: 1
                TR(e1/1/4) SG : J(185) ET: 210, Up Time: 00:02:52
```

The following example shows PIM SM information for a VLAN.

```
Device#show ipv6 pimsm-snooping vlan 503
OIF Info:
TR - OIF Belongs to Trunk/LAG, Primary port is displayed
SG - (s,g) downstream fsm state:
G - (*,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

PIMSM Snoop cache for vlan 503
1    (* ff7e::1:2:3) Up Time: 03:43:46
                OIF: 1
                TR(e1/1/4) G : J(177) ET: 210, Up Time: 03:43:46

2    (3000::10 ff7e::1:2:3) Up Time: 00:02:58
                OIF: 1
                TR(e1/1/4) SG : J(179) ET: 210, Up Time: 00:02:58
```

The following example shows PIM SM resource information.

```
Device#show ipv6 pimsm-snooping resources
                      alloc in-use  avail get-fail    limit  get-mem  size init
pimsm group entry      1000      1    999        0   232000        2    64 1000
pimsm source entry     2000      1   1999        0   464000        2    68 2000
pimsm oif entry        2000      1   1999        0   464000        2    89 2000

Total memory in used: 378000 bytes
```

show ipv6 raguard

Displays the Router Advertisement (RA) guard configuration details.

Syntax

show ipv6 raguard { **counts** | **policy** } { *name* | **all** }

show ipv6 raguard whitelist { *number* | **all** }

Parameters

counts

Displays the RA guard permit or drop counts.

policy

Displays the RA guard policy details.

whitelist

Displays the RA guard whitelist associated with the RA guard policy.

name

An ASCII string indicating the name of the RA guard policy, when used along with **counts** keyword, displays the permit or drop counts for the specified RA guard policy. When used with **policy** keyword, displays the configuration of the specified RA guard policy.

all

When used with **counts**, **policy**, and **whitelist** keywords, displays the permit or drop counts for all the RA guard policies, configuration of all RA guard policies, and all the associated RA guard whitelists respectively.

number

Displays the specific whitelist based on the ID number.

Modes

Privileged EXEC mode

Global configuration mode

Usage Guidelines

The **show ipv6 raguard counts** command is applicable only when logging is enabled on the policy.

Examples

The following example shows the RA guard drop or permit counts for all RA guard policies:

```
device#show ipv6 raguard counts all
POLICY: policy1
DROPPED-host port: 1
DROPPED-whitelist: 4
DROPPED-prefixlist: 1
DROPPED-max pref: 3
PASSED-trusted port: 0
PASSED-untrusted port: 0
POLICY: policy2
DROPPED-host port: 1
DROPPED-whitelist: 0
DROPPED-prefixlist: 3
DROPPED-max pref: 1
PASSED-trusted port: 0
PASSED-untrusted port: 0
```

The following example shows the details of a RA guard policy p1:

```
device#show ipv6 raguard policy p1
policy:p1
        whitelist:1
```

The following example shows all RA guard whitelist:

```
device#show ipv6 raguard whitelist all
whitelist #1 : 3 entries
        permit fe80:db8::db8:10/128
        permit fe80:db8::db8:5/128
        permit fe80:db8::db8:12/128
```

show ipv6 static mroute

Displays information for configured IPv6 multicast routes.

Syntax

show ipv6 static mroute [**vrf** *vrf-name* | *ipv6-address-prefix/prefix-length*]

Parameters

vrf *vrf-name*
Specifies a VRF route.

ipv6-address-prefix/prefix-length
Specifies an IPv6 address.

Modes

Privileged EXEC mode

Global configuration mode

Usage Guidelines

Only resolved and best static mroutes are added to the mRTM table. These routes are prefixed with an asterisk in the output from the **show ipv6 static mroute** command.

Examples

Thie following example displays information for configured IPv6 multicast routes:

```
Device(config)# show ipv6 static mroute
IPv6 Static Routing Table - 1 entries:
 IPv6 Prefix                    Interface  Next Hop Router      Met/Dis/Tag Name
*1:1::1:0/120                   ve 90      ::                   1/1/0
```

History

Release version	Command history
8.0.10a	This command was introduced.

show ipv6 tunnel

Displays a summary of tunnel information.

Syntax

show ipv6 tunnel [**config**]

Parameters

config

Displays IPv6 tunnel configurations.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show ipv6 tunnel** command displays the following information:

Output field	Description
Tunnel	The tunnel interface number.
Mode	The tunnel mode. Possible modes include the following: • configured - Indicates a manually configured tunnel.
Packet Received	The number of packets received by a tunnel interface. Note that this is the number of packets received by the CPU. It does not include the number of packets processed in hardware.
Packet Sent	The number of packets sent by a tunnel interface. Note that this is the number of packets sent by the CPU. It does not include the number of packets processed in hardware.

Examples

The following is a sample output of the **show ipv6 tunnel** command.

```
device# show ipv6 tunnel

IP6 Tunnels
Tunnel        Mode        Tunnel Status Packet Received    Packet Sent
1               configured     Active           0                              0
2               configured     Active           0                              22419
```

show lag

Displays Link Aggregation Group (LAG) information.

Syntax

show lag [*lag-name* | **brief** | **deployed** | **dynamic** | **id** *number* | **keep-alive** | **static**]

Parameters

lag-name
Displays the LAG specified by the LAG name.

brief
Displays the LAG information summary.

deployed
Displays information about all the deployed LAGs.

dynamic
Displays information about dynamic LAGs.

id *number*
Displays information about the LAG specified by the ID number.

keep-alive
Displays information about keep-alive LAGs.

static
Displays information about static LAGs.

Modes

User EXEC mode

Privileged EXEC mode

LAG configuration mode

Command Output

The **show lag** command displays the following information:

Output field	Description
Total number of LAGS	The total number of LAGs that have been configured on the device.
Total number of deployed LAGS	The total number of LAGs on the device that are currently deployed.
Total number of trunks created	The total number of trunks that have been created on the LAG. The total number of LAGs available are shown also. Because keep-alive LAGs do not use LAG IDs, they are not listed and do not subtract from the number of LAGs available.
LACP System Priority /ID	The system priority configured for the device. The ID is the system priority that is the base MAC address of the device.

Output field	Description
LACP Long timeout	The number of seconds used for the LACP long timeout mode. This is only applicable for dynamic or keep-alive LAGs.
LACP Short timeout	The number of seconds used for the LACP short timeout mode. This is only applicable for dynamic or keep-alive LAGs.

The following information is displayed per-LAG in the **show lag brief** command:

Output field	Description
LAG	The name of the LAG, LAG ID number, the configured type of the LAG: static, dynamic, or keep-alive, status of LAG deployment: deployed or not.

The following information is displayed per-LAG in the **show lag** command for each LAG configured:

Output field	Description
LAG Configuration	
Ports	List of ports configured with the LAG.
Port Count	Number of ports configured on the LAG.
Primary Port	The primary port configured on the LAG.
Trunk Type	The load sharing method configured for the LAG: hash-based.
LACP Key	The link aggregation key for the LAG.

The following information is displayed for the **show lag deployed** command:

Output field	Description
Deployment	
LAG ID	The LAG ID number.
Active Primary	The port within the LAG where most protocol packets are transmitted. This is not the same as the configured Primary Port of the LAG.
Port	The chassis slot and port number of the interface.
Link	The status of the link, which can be one of the following: • up • down
State	The Layer 2 state for the port.
Dupl	The duplex state of the port, which can be one of the following: • Full • Half • None
Speed	The bandwidth of the interface.
Trunk	The LAG ID of the port.
Tag	Indicates whether the ports have 802.1q VLAN tagging. The value can be Yes or No.
Pri	Indicates the Quality of Service (QoS) priority of the ports. The priority can be a value from 0 through 7.
MAC	The MAC address of the port.
Name	The name (if any) configured for the port.

Output field	Description
Sys P	Lists the system priority configured for the device.
Port P	Lists the port's link aggregation priority.
Key	Lists the link aggregation key.
Act	Indicates the link aggregation mode, which can be one of the following: • No: The mode is passive on the port. If link aggregation is enabled (and the mode is passive), the port can send and receive LACPDU messages to participate in negotiation of an aggregate link initiated by another port, but cannot search for a link aggregation port or initiate negotiation of an aggregate link. • Yes: The mode is active. The port can send and receive LACPDU messages.
Tio	Indicates the timeout value of the port. The timeout value can be one of the following: • L: Long. The LAG group has already been formed and the port is therefore using a longer message timeout for the LACPDU messages exchanged with the remote port. Typically, these messages are used as confirmation of the health of the aggregate link. • S: Short. The port has just started the LACPDU message exchange process with the port at the other end of the link. The S timeout value also can mean that the link aggregation information received from the remote port has expired and the ports are starting a new information exchange.
Agg	Indicates the link aggregation state of the port. The state can be one of the following: • Agg: Link aggregation is enabled on the port. • No: Link aggregation is disabled on the port.
Syn	Indicates the synchronization state of the port. The state can be one of the following: • No: The port is out of sync with the remote port. The port does not understand the status of the LACPDU process and is not prepared to enter a LAG link. • Syn: The port is in sync with the remote port. The port understands the status of the LACPDU message exchange process, and therefore knows the LAG group to which it belongs, the link aggregation state of the remote port, and so on.
Dis	Indicates the collection state of the port, which determines whether the port is ready to send traffic over the LAG link: • Col: The port is ready to send traffic over the LAG link. • No: The port is not ready to send traffic over the LAG link.
Col	Indicates the distribution state of the port, which determines whether the port is ready to receive traffic over the LAG link: • Dis: The port is ready to receive traffic over the LAG link. • No: The port is not ready to receive traffic over the LAG link.
Def	Indicates whether the port is using default link aggregation values. The port uses default values if it has not received link aggregation information through LACP from the port at the remote end of the link. This field can have one of the following values: • Def: The port has not received link aggregation values from the port at the other end of the link and is therefore using its default link aggregation LACP settings. • No: The port has received link aggregation information from the port at the other end of the link and is using the settings negotiated with that port.
Exp	Indicates whether the negotiated link aggregation settings have expired. The settings expire if the port does not receive an LACPDU message from the port at the other end of the link before the message timer expires. This field can have one of the following values: • Exp: The link aggregation settings this port negotiated with the port at the other end of the link have expired. The port is now using its default link aggregation settings. • No: The link aggregation values that this port negotiated with the port at the other end of the link have not expired. The port is still using the negotiated settings.

Output field	Description
Ope	• Ope (operational): The port is operating normally. • Blo (blocked): The port is blocked because the adjacent port is not configured with link aggregation or because it is not able to join a LAG. An LACP port is blocked until it becomes part of a LAG. Also, an LACP port is blocked if its state becomes "default". To unblock the port and bring it to an operational state, enable link aggregation on the adjacent port and ensure that the ports have the same key. • Frc (force-up): The port is in "force-up" mode. If you have configured the **force-up ethernet** command on the member port of a dynamic LAG, the port goes into "force-up" mode and is logically operational when the dynamic LAG is not operating. • Err: If there is a peer information mismatch, then that particular port is moved to the Error disable state (Err).
Port	The chassis slot and port number of the interface.
Partner System ID	The partner system ID indicating the system's priority and the MAC address of the port.
Partner Key	The partner key value. Valid key values range from 1 to 65535.
LACP Rx Count	This is the counter for LACPDUs received on this port.
LACP Tx Count	This is the counter for LACPDUs transmitted from this port.

Examples

The following example shows sample output of the **show lag** command.

```
device(config)# show lag
Total number of LAGs:          5
Total number of deployed LAGs: 3
Total number of trunks created:2 (253 available)
LACP System Priority / ID:     1 / 0024.3889.3b00
LACP Long timeout:             120, default: 120
LACP Short timeout:            3, default: 3
=== LAG "test" ID 35 (static Deployed) ===
LAG Configuration:
   Ports:         e 1/3/10
   Port Count:    1
   Primary Port:  1/3/10
   Trunk Type:    hash-based
Deployment: HW Trunk ID 1
Port      Link    State   Dupl Speed Trunk Tag Pvid Pri MAC            Name
1/3/10    Down    None    None None  35    No  1    0   0024.3889.3b09
=== LAG "test2" ID 1 (static Deployed) ===
LAG Configuration:
   Ports:         e 1/3/11
   Port Count:    1
   Primary Port:  1/3/11
   Trunk Type:    hash-based
Deployment: HW Trunk ID 2
Port    Link    State   Dupl Speed Trunk Tag Pvid Pri MAC            Name
3/11    Down    None    None None  1     No  1    0   0024.3889.3b0a
=== LAG "test3" (keep-alive Deployed) ===
LAG Configuration:
   Ports:         e 1/3/12
   Port Count:    1
   Primary Port:  1/3/12
   Trunk Type:    hash-based
   LACP Key:      9860
Deployment:
Port      Link    State   Dupl Speed Trunk Tag Pvid Pri MAC            Name
1/3/12    Down    None    None None  None  No  1    0   0024.3889.3b0b
Port   [Sys P] [Port P] [ Key ] [Act][Tio][Agg][Syn][Col][Dis][Def][Exp][Ope]
1/3/12     1        1    9860   Yes   S   Agg  Syn  No   No   Def  No   Dwn
Partner Info and PDU Statistics
Port       Partner         Partner     LACP      LACP
           System MAC         Key     Rx Count  Tx Count
1/3/12     0000.0000.0000      139        0         0

=== LAG "test4" (keep-alive Not Deployed) ===
LAG Configuration:
   Ports:         e 1/3/13
   Port Count:    1
   Primary Port:  1/3/13
   Trunk Type:    hash-based
   LACP Key:      0
=== LAG "test5" ID 2 (static Not Deployed) ===
LAG Configuration:
   Ports:         e 1/3/14
   Port Count:    1
   Primary Port:  none
   Trunk Type:    hash-based
   Hardware failover mode:     all-ports
```

The following example shows sample output of the **show lag deployed** command.

```
device(config)# show lag R4-dyn2
Total number of LAGs:          3
Total number of deployed LAGs: 2
Total number of trunks created:2 (122 available)
LACP System Priority / ID:     1 / 7e8e.f82d.8040
LACP Long timeout:             120, default: 120
LACP Short timeout:            3, default: 3

=== LAG "R4-dyn2" ID 200 (dynamic Deployed) ===
LAG Configuration:
   Ports:         e 2/1/11 to 2/1/12
   Port Count:    2
   Primary Port:  2/1/11
   Trunk Type:    hash-based
   LACP Key:      20200
Deployment: HW Trunk ID 2
Port       Link    State   Dupl Speed Trunk Tag Pvid Pri MAC             Name
2/1/11     Up      Forward Full 1G    200   Yes N/A  0   7e8e.f82d.8040
2/1/12     Up      Forward Full 1G    200   Yes N/A  0   7e8e.f82d.8040

Port       [Sys P] [Port P] [ Key ] [Act][Tio][Agg][Syn][Col][Dis][Def][Exp][Ope]
2/1/11          1        1   20200   Yes   L   Agg  Syn  Col  Dis  No   No   Ope
2/1/12          1        1   20200   Yes   L   Agg  Syn  Col  Dis  No   No   Ope


 Partner Info and PDU Statistics
Port          Partner         Partner     LACP      LACP
             System ID         Key     Rx Count  Tx Count
2/1/11   1-0024.3821.5600      480        6         268
2/1/12   1-0024.3821.5600      480        8         267
```

History

Release version	Command history
8.0.30d	This command was modified to display a changed output for the **deployed** keyword.

show link-error-disable

Displays the ports with the port flap dampening feature enabled.

Syntax

show link-error-disable [**all**]

Parameters

all

Displays all the ports with the port flap dampening feature enabled.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

Ports that have been disabled due to the port flap dampening feature are identified in the output of the **show link-error-disable** command.

Command Output

The **show link-error-disable** command displays the following information:

Output field	Description
Port	Specifies the port number.
threshold	The number of times the port link state will go from up to down and down to up before the wait period is activated.
sampling-period	The number of seconds during which the specified toggle threshold can occur before the wait period is activated.
waiting-time	The number of seconds the port remains disabled (down) before it becomes enabled.

Examples

The following is a sample output of the **show link-error-disable all** command.

```
device# show link-error-disable all

Port1/1/1 is configured for link-error-disable
            threshold:1, sampling_period:10, waiting_period:0
Port1/1/2 is configured for link-error-disable
            threshold:1, sampling_period:10, waiting_period:0
Port1/1/3 is configured for link-error-disable
            threshold:1, sampling_period:10, waiting_period:0
Port1/1/4 is configured for link-error-disable
            threshold:1, sampling_period:10, waiting_period:0
Port1/1/5 is configured for link-error-disable
            threshold:4, sampling_period:10, waiting_period:2
Port1/1/9 is configured for link-error-disable
            threshold:2, sampling_period:20, waiting_period:0
```

show link-keepalive

Displays the UDLD information.

Syntax

show link-keepalive [**ethernet** *stackid/slot/port*]

Parameters

ethernet *stackid/slot/port*

Displays UDLD information for the specified Ethernet port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show link-keepalive** command displays the following information:

Output field	Description
Total link-keepalive enabled ports	The total number of ports on which UDLD is enabled.
Keepalive Retries	The number of times a port will attempt the health-check before concluding that the link is down.
Keepalive Interval	The number of seconds between health check packets.
Port	The port number.
Physical Link	The state of the physical link. This is the link between the Brocade port and the directly connected device.
Logical Link	The state of the logical link. This is the state of the link between this Brocade port and the Brocade port on the other end of the link.
State	The traffic state of the port.
Link-vlan	The ID of the tagged VLAN in the UDLD packet.

The **show link-keepalive ethernet** command displays the following information:

Output field	Description
Current State	The state of the logical link. This is the link between this Brocade port and the Brocade port on the other end of the link.
Remote MAC Addr	The MAC address of the port or device at the remote end of the logical link.
Local Port	The port number on this Brocade device.
Remote Port	The port number on the Brocade device at the remote end of the link.
Local System ID	A unique value that identifies this Brocade device. The ID can be used by Brocade technical support for troubleshooting.

Output field	Description
Remote System ID	A unique value that identifies the Brocade device at the remote end of the link.
Packets sent	The number of UDLD health-check packets sent on this port.
Packets received	The number of UDLD health-check packets received on this port.
Transitions	The number of times the logical link state has changed between up and down.
Port blocking	Information used by Brocade technical support for troubleshooting.
Link-vlan	The ID of the tagged VLAN in the UDLD packet.
BM disabled	Information used by Brocade technical support for troubleshooting.

Examples

The following example shows the UDLD information for all ports.

```
device# show link-keepalive
Total link-keepalive enabled ports: 4
Keepalive Retries: 3    Keepalive Interval: 1 Sec.
Port    Physical Link   Logical Link    State           Link-vlan
1/1/1     up              up            FORWARDING      3
1/1/2     up              up            FORWARDING
1/1/3     down            down          DISABLED
1/1/4     up              down          DISABLED
```

The following example show the UDLD information for a specific port.

```
device# show link-keepalive ethernet 1/4/1
Current State   : up            Remote MAC Addr  : 0000.00d2.5100
Local Port      : 1/4/1         Remote Port      : 1/2/1
Local System ID : e0927400      Remote System ID : e0d25100
Packets sent    : 254           Packets received : 255
Transitions     : 1             Link-vlan        : 100
```

show link-oam info

Displays the OAM information on EFM-OAM-enabled ports.

Syntax

show link-oam info [**detail** [**ethernet** *stackid/slot/port* [[**to** *stackid/slot/port*] [**ethernet** *stackid/slot/port*]...]]]

Parameters

detail

Displays detailed EFM-OAM information.

ethernet

Displays the detailed EFM-OAM information for a specific Ethernet interface.

stackid/slot/port

Specifies the interface details.

to

Configures a range of interfaces.

Modes

Privileged EXEC mode

Global configuration mode

EFM-OAM protocol configuration mode

Command Output

The **show link-oam info** command displays the following information:

Output field	Description
Ethernet	Displays the interface details
Link Status	Displays the status of the link (up or down)
OAM Status	Displays the status of OAM
Mode	Displays the operational mode of EFM-OAM
Local Stable	Displays the local OAM status
Remote Stable	Displays the remote OAM status
multiplexer action	Displays the local/remote multiplexer action
parse action	Displays the local/remote parse action
stable	Displays the local/remote OAM status
state	Displays the local/remote EFM-OAM state
loopback support	Indicates whether there is support for loopback for remote/local
dying-gasp	Indicates whether there is support for dying gasp for remote/local
critical-event	Indicates whether there is support for critical-event for remote/local

Output field	Description
link-fault	Indicates whether there is support for link-fault for remote/local

Examples

The following example displays the OAM information on all EFM-OAM-enabled ports.

```
device(config)# show link-oam info
Ethernet Link Status     OAM Status      Mode       Local Stable    Remote Stable
1/1/1    up              up              active     satisfied       satisfied
1/1/2    up              up              passive    satisfied       satisfied
1/1/3    up              up              active     satisfied       satisfied
1/1/4    up              init            passive    unsatisfied     unsatisfied
1/1/5    down            down            passive    unsatisfied     unsatisfied
1/1/6    down            down            passive    unsatisfied     unsatisfied
1/1/7    down            down            passive    unsatisfied     unsatisfied
```

The following example displays detailed EFM-OAM information on all EFM-OAM-enabled ports.

```
device(config)# show link-oam info detail
OAM information for Ethernet port: 10/1/1
        +link-oam mode:        passive
        +link status:          down
        +oam status:           down
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                state:               linkFault
                loopback state:      disabled
                dying-gasp:          false
                critical-event:      false
                link-fault:          true
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                loopback support:    disabled
                dying-gasp:          false
                critical-event:      true
                link-fault:          false

OAM information for Ethernet port: 10/1/3
        +link-oam mode:        active
        +link status:          up
        +oam status:           down
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                state:               activeSend
                loopback state:      disabled
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                loopback support:    disabled
                dying-gasp:          false
                critical-event:      false
                link-fault:          false

OAM information for Ethernet port: 10/1/4
        +link-oam mode:        active
        +link status:          up
        +oam status:           up
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              satisfied
                state:               up
                loopback state:      disabled
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              satisfied
                loopback support:    disabled
                dying-gasp:          false
                critical-event:      true
                link-fault:          false
```

The following example displays detailed EFM-OAM information on a range of EFM-OAM-enabled ports.

```
device(config)# show link-oam info detail ethernet 1/1/3 to 1/1/8
OAM information for Ethernet port: 1/1/3
        +link-oam mode:        active
        +link status:          up
        +oam status:           up
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              satisfied
                state:               up
                loopback state:      disabled
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              satisfied
                loopback support:    disabled
                dying-gasp:          false
                critical-event:      false
                link-fault:          false

Link OAM is not enabled on port 1/1/4
Link OAM is not enabled on port 1/1/5
Link OAM is not enabled on port 1/1/6
Link OAM is not enabled on port 1/1/7
Link OAM is not enabled on port 1/1/8
```

History

Release version	Command history
08.0.30	This command was introduced.

show link-oam statistics

Displays the OAM statistics of OAM-enabled ports.

Syntax

show link-oam statistics [**detail** [**ethernet** *stackid/slot/port* [[**to** *stackid/slot/port*] [**ethernet** *stackid/slot/port*]...]]]

Parameters

detail

Displays detailed EFM-OAM statistics.

ethernet

Displays the detailed EFM-OAM statistics of a specific ethernet interface.

stackid/slot/port

Specifies the interface details.

to

Configures a range of interfaces.

Modes

Privileged EXEC mode

Global configuration mode

EFM-OAM protocol configuration mode

Command Output

The **show link-oam statistics** command displays the following information:

Output field	Description
Tx PDUs	Displays the number of PDUs transmitted
Rx PDUs	Displays the number of PDUs received
information OAMPDUs	Displays the number of information OAMPDUs transmitted/received
loopback control OAMPDUs	Displays the number of loopback control OAMPDUs transmitted/received
variable request OAMPDUs	Displays the number of variable request OAMPDUs transmitted/received
variable response OAMPDUs	Displays the number of variable response OAMPDUs transmitted/received
unique event notification OAMPDUs	Displays the number of unique event notification OAMPDUs transmitted/received
duplicate event notification OAMPDUs	Displays the number of duplicate event notification OAMPDUs transmitted/received
organization specific OAMPDUs	Displays the number of organization specific OAMPDUs transmitted/received
link-fault records	Displays the number of link-fault records transmitted/received
critical-event records	Displays the number of critical-event records transmitted/received
dying-gasp records	Displays the number of dying-gasp records transmitted/received
loopback control OAMPDUs dropped	Displays the number of dropped loopback control OAMPDUs

Output field	Description
unsupported OAMPDUs	Displays the number of unsupported OAMPDUs
discarded TLVs	Displays the number of discarded TLVs
unrecognized TLVs	Displays the number of unrecognized TLVs

Examples

The following example displays the OAM statistics on all EFM-OAM-enabled ports.

```
device(config)# show link-oam statistics
Ethernet Tx Pdus         Rx Pdus
10/1/1   377908         377967
10/1/3   400            44
10/1/4   400            385
10/1/5   400            385
10/1/6   400            385
```

The following example displays detailed EFM-OAM statistics on all EFM-OAM-enabled ports.

```
device(config)# show link-oam statistics detail
OAM statistics for Ethernet port: 10/1/1
        Tx statistics
                information OAMPDUs:                    377908
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
        Rx statistics
                information OAMPDUs:                    377967
                loopback control OAMPDUs:               0
                loopback control OAMPDUs dropped:       0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                unsupported OAMPDUs:                    0
                link-fault records:                     0
                critical-event records:                 377395
                dying-gasp records:                     0
                discarded TLVs:                         0
                unrecognized TLVs:                      0

OAM statistics for Ethernet port: 10/1/3
        Tx statistics
                information OAMPDUs:                    427
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
        Rx statistics
                information OAMPDUs:                    44
                loopback control OAMPDUs:               0
                loopback control OAMPDUs dropped:       0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                unsupported OAMPDUs:                    0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
                discarded TLVs:                         0
                unrecognized TLVs:                      0

OAM statistics for Ethernet port: 10/1/4
        Tx statistics
                information OAMPDUs:                    428
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
```

```
        Rx statistics
                information OAMPDUs:                    413
                loopback control OAMPDUs:               0
                loopback control OAMPDUs dropped:       0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                unsupported OAMPDUs:                    0
                link-fault records:                     0
                critical-event records:                 350
                dying-gasp records:                     0
                discarded TLVs:                         0
                unrecognized TLVs:                      0
```

The following example displays detailed EFM-OAM statistics on a range of EFM-OAM-enabled ports.

```
device(config)# show link-oam statistics detail ethernet 1/1/3 to 1/1/8
OAM statistics for Ethernet port: 1/1/3
        Tx statistics
                information OAMPDUs:                    255390
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
        Rx statistics
                information OAMPDUs:                    282796
                loopback control OAMPDUs:               0
                loopback control OAMPDUs dropped:       0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                unsupported OAMPDUs:                    0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
                discarded TLVs:                         0
                unrecognized TLVs:                      0

Link OAM is not enabled on port 1/1/4
Link OAM is not enabled on port 1/1/5
Link OAM is not enabled on port 1/1/6
Link OAM is not enabled on port 1/1/7
Link OAM is not enabled on port 1/1/8
```

History

Release version	Command history
08.0.30	This command was introduced.

show lldp

Displays a summary of the LLDP configuration settings.

Syntax

show lldp

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show lldp** command displays the following information:

Output field	Description
LLDP transmit interval	The number of seconds between regular LLDP packet transmissions.
LLDP transmit hold multiplier	The multiplier used to compute the actual time-to-live (TTL) value of an LLDP advertisement. The TTL value is the transmit interval multiplied by the transmit hold multiplier.
LLDP transmit delay	The number of seconds the LLDP agent will wait after transmitting an LLDP frame and before transmitting another LLDP frame.
LLDP SNMP notification interval	The number of seconds between transmission of SNMP LLDP traps (lldpRemTablesChange) and SNMP LLDP-MED traps (lldpXMedTopologyChangeDetected).
LLDP reinitialize delay	The minimum number of seconds the device will wait from when LLDP is disabled on a port, until a request to re-enable LLDP on that port will be honored.
LLDP-MED fast start repeat count	The number of seconds between LLDP frame transmissions when an LLDP-MED Endpoint is newly detected.
LLDP maximum neighbors	The maximum number of LLDP neighbors for which LLDP data will be retained, per device.
LLDP maximum neighbors per port	The maximum number of LLDP neighbors for which LLDP data will be retained, per port.

Examples

The following is a sample output of the **show lldp** command.

```
device# show lldp

LLDP transmit interval                      : 10 seconds
LLDP transmit hold multiplier    : 4 (transmit TTL: 40 seconds)
LLDP transmit delay              : 1 seconds
LLDP SNMP notification interval     : 5 seconds
LLDP reinitialize delay          : 1 seconds
LLDP-MED fast start repeat count    : 3
LLDP maximum neighbors                      : 392
LLDP maximum neighbors per port     : 4
```

show lldp local-info

Displays the details of the LLDP advertisements that will be transmitted on each port.

Syntax

show lldp local-info ports { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]}

Parameters

ports
: Displays the details of the LLDP advertisements that will be transmitted on the specified port.

all
: Displays the details of the LLDP advertisements that will be transmitted on all LLDP enabled ports.

ethernet *stackid/slot/port*
: Displays the details of the LLDP advertisements that will be transmitted on the specified ethernet port.

to *stackid/slot/port*
: Displays the details of the LLDP advertisements that will be transmitted on a range of ports.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

The contents of the show output will vary depending on which TLVs are configured to be advertised.

If you do not specify any ports or use the keyword all , by default, the report will show the local information advertisements for all ports.

Examples

The following is a sample output of the **show lldp local-info** command.

```
device# show lldp local-info

Local port: 1/1/9:1
  + Chassis ID (MAC address): 0000.0043.4343
  + Port ID (MAC address): cc4e.2438.3294
  + Time to live: 120 seconds
  + System name         : "775026Q-Seth"
  + Port description    : "10GigabitEthernet1/1/9:1"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation supported, but disabled
    Operational MAU type   : Other
  + Link aggregation: aggregated (aggregated port ifIndex: 21)
  + Maximum frame size: 10200 octets
  + Port VLAN ID: none
  + Management address (IPv4): 10.37.160.43

Local port: 1/1/9:2
  + Chassis ID (MAC address): 0000.0043.4343
  + Port ID (MAC address): cc4e.2438.3295
  + Time to live: 120 seconds
  + System name         : "775026Q-Seth"
  + Port description    : "10GigabitEthernet1/1/9:2"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation not supported
    Operational MAU type   : 77
  + Link aggregation: aggregated (aggregated port ifIndex: 21)
  + Maximum frame size: 10200 octets
  + Port VLAN ID: none
  + Management address (IPv4): 10.37.160.43

Local port: 1/1/9:3
  + Chassis ID (MAC address): 0000.0043.4343
  + Port ID (MAC address): cc4e.2438.3296
  + Time to live: 120 seconds
  + System name         : "775026Q-Seth"
  + Port description    : "10GigabitEthernet1/1/9:3"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation not supported
    Operational MAU type   : 162
  + Link aggregation: aggregated (aggregated port ifIndex: 21)
  + Maximum frame size: 10200 octets
  + Port VLAN ID: none
  + Management address (IPv4): 10.37.160.43

Local port: 1/1/9:4
  + Chassis ID (MAC address): 0000.0043.4343
  + Port ID (MAC address): cc4e.2438.3297
  + Time to live: 120 seconds
  + System name         : "775026Q-Seth"
  + Port description    : "10GigabitEthernet1/1/9:4"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation not supported
    Operational MAU type   : b10G1GbasePRXD1
  + Link aggregation: aggregated (aggregated port ifIndex: 21)
  + Maximum frame size: 10200 octets
  + Port VLAN ID: none
  + Management address (IPv4): 10.37.160.43

Local port: 1/1/11:1
  + Chassis ID (MAC address): 0000.0043.4343
  + Port ID (MAC address): cc4e.2438.329c
  + Time to live: 120 seconds
  + System name         : "775026Q-Seth"
```

```
  + Port description    : "10GigabitEthernet1/1/11:1"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation supported, but disabled
    Operational MAU type   : Other
  + Link aggregation: aggregated (aggregated port ifIndex: 29)
  + Maximum frame size: 10200 octets
  + Port VLAN ID: none
  + Management address (IPv4): 10.37.160.43

Local port: 1/1/11:2
  + Chassis ID (MAC address): 0000.0043.4343
  + Port ID (MAC address): cc4e.2438.329d
  + Time to live: 120 seconds
  + System name         : "775026Q-Seth"
  + Port description    : "10GigabitEthernet1/1/11:2"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation not supported
    Operational MAU type   : 162
  + Link aggregation: aggregated (aggregated port ifIndex: 29)
  + Maximum frame size: 10200 octets
  + Port VLAN ID: none
  + Management address (IPv4): 10.37.160.43

Local port: 1/1/11:3
  + Chassis ID (MAC address): 0000.0043.4343
  + Port ID (MAC address): cc4e.2438.329e
  + Time to live: 120 seconds
  + System name         : "775026Q-Seth"
  + Port description    : "10GigabitEthernet1/1/11:3"
  + System capabilities : bridge, router
    Enabled capabilities: bridge, router
  + 802.3 MAC/PHY          : auto-negotiation not supported
    Operational MAU type   : b10G1GbasePRXD1
  + Link aggregation: aggregated (aggregated port ifIndex: 29)
  + Maximum frame size: 10200 octets
  + Port VLAN ID: none
  + Management address (IPv4): 10.37.160.43

<<output truncated>>
```

show lldp neighbors

Displays a list of current LLDP neighbors and details of the latest advertisements received from LLDP neighbors.

Syntax

show lldp neighbors [**detail ports** { **all** | **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...] }]

Parameters

detail

Displays detailed neighbor data.

ports

Displays the details of the latest advertisements received from LLDP neighbors for the specified port.

ethernet *stackid/slot/port*

Displays the details of the latest advertisements received from LLDP neighbors for the specified Ethernet port.

all

Displays the details of the latest advertisements received from LLDP neighbors for all LLDP enabled ports.

to *stackid/slot/port*

Displays the details of the latest advertisements received from LLDP neighbors for a range of ports.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show lldp neighbors** command displays the following information:

Output field	Description
Lcl Port	The local LLDP port number.
Chassis ID	The identifier for the chassis. Brocade devices use the base MAC address of the device as the Chassis ID.
Port ID	The identifier for the port. Brocade devices use the permanent MAC address associated with the port as the port ID.
Port Description	The description for the port. Brocade devices use the ifDescr MIB object from MIB-II as the port description.
System Name	The administratively-assigned name for the system. Brocade devices use the sysName MIB object from MIB-II, which corresponds to the CLI **hostname** command setting.

Examples

The following example is a sample output of the **show lldp neighbors** command.

```
device# show lldp neighbors

Lcl Port Chassis ID      Port ID         Port Description            System Name
1/1/9:1  0000.0126.2057  748e.f8f9.7489  10GigabitEthernet1/1/10     7750Stk
1/1/9:2  0000.0126.2057  748e.f8f9.7509  10GigabitEthernet2/1/10     7750Stk
1/1/9:3  0000.0126.2057  748e.f8f9.7488  10GigabitEthernet1/1/9      7750Stk
1/1/9:4  0000.0126.2057  748e.f8f9.7508  10GigabitEthernet2/1/9      7750Stk
1/1/11:1 0000.4690.5353  cc4e.246c.e5a2  10GigabitEthernet1/2/2      7450Stk
1/1/11:2 0000.4690.5353  cc4e.246c.ea41  10GigabitEthernet2/2/1      7450Stk
1/1/11:3 0000.4690.5353  cc4e.246c.e5a1  10GigabitEthernet1/2/1      7450Stk
1/1/11:4 0000.4690.5353  cc4e.246c.df21  10GigabitEthernet3/2/1      7450Stk
```

The following example is a sample output of the **show lldp neighbors detail** command.

```
device# show lldp neighbors detail ports ethernet 1/1/9:1

Local port: 1/1/9:1
  Neighbor: 748e.f8f9.7489, TTL 92 seconds
    + Chassis ID (MAC address): 0000.0126.2057
    + Port ID (MAC address): 748e.f8f9.7489
    + Time to live: 120 seconds
    + System name         : "7750Stk-Seth"
    + Port description    : "10GigabitEthernet1/1/10"
    + System capabilities : bridge, router
      Enabled capabilities: bridge, router
    + 802.3 MAC/PHY          : auto-negotiation supported, but disabled
      Operational MAU type   : Other
    + Link aggregation: aggregated (aggregated port ifIndex: 10)
    + Maximum frame size: 10200 octets
    + Port VLAN ID: none
    + Management address (IPv4): 10.37.160.126
```

show lldp statistics

Displays LLDP global and per-port statistics.

Syntax

show lldp statistics

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example is a sample output of the **show lldp statistics** command.

```
device# show lldp statistics

Last neighbor change time: 3 hour(s) 37 minute(s) 59 second(s) ago

Neighbor entries added          : 25
Neighbor entries deleted        : 17
Neighbor entries aged out       : 3
Neighbor advertisements dropped : 0

Port       Tx Pkts   Rx Pkts   Rx Pkts   Rx Pkts   Rx TLVs   Rx TLVs Neighbors
             Total     Total  w/Errors Discarded Unrecognz Discarded  Aged Out
1/1/1            0         0         0         0         0         0         0
1/1/2            0         0         0         0         0         0         0
1/1/3            0         0         0         0         0         0         0
1/1/4            0         0         0         0         0         0         0
1/1/5            0         0         0         0         0         0         0
1/1/6            0         0         0         0         0         0         0
1/1/7            0         0         0         0         0         0         0
1/1/8            0         0         0         0         0         0         0
1/1/9:1        523       522         0         0         0         0         0
1/1/9:2        475       476         0         0         0         0         1
1/1/9:3        476       476         0         0         0         0         1
1/1/9:4        475       477         0         0         0         0         1
1/1/10           0         0         0         0         0         0         0
1/1/11:1       510       524         0         0         0         0         0
1/1/11:2       510       524         0         0         0         0         0
1/1/11:3       511       525         0         0         0         0         0
1/1/11:4       510       524         0         0         0         0         0
1/1/12           0         0         0         0         0         0         0
1/1/13           0         0         0         0         0         0         0
1/1/14           0         0         0         0         0         0         0
1/1/15           0         0         0         0         0         0         0
1/1/16           0         0         0         0         0         0         0
1/1/17           0         0         0         0         0         0         0
1/1/18           0         0         0         0         0         0         0
1/1/19           0         0         0         0         0         0         0
1/1/20           0         0         0         0         0         0         0
1/2/1            0         0         0         0         0         0         0
1/2/2            0         0         0         0         0         0         0
1/2/3            0         0         0         0         0         0         0
1/2/4            0         0         0         0         0         0         0
1/2/5            0         0         0         0         0         0         0
1/2/6            0         0         0         0         0         0         0
1/3/1            0         0         0         0         0         0         0
1/3/2            0         0         0         0         0         0         0
1/3/3            0         0         0         0         0         0         0
1/3/4            0         0         0         0         0         0         0
1/3/5            0         0         0         0         0         0         0
1/3/6            0         0         0         0         0         0         0
```

show local-userdb

Displays a list of local user databases configured on the device and the number of users in each database.

Syntax

show local-userdb [*db-name* [*user-name*]]

Parameters

db-name

Displays information for the specified local user database. The database name and the username can be up to 31 characters.

user-name

Displays information for the specified user in the specified user database.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Web Authentication configuration mode

Examples

The following example displays the list of all local user databases and the number of users in each database.

```
device# show local-userdb
==========================================================================
Local User Database Name : My_Database
Number of users in the database : 4
==========================================================================
Local User Database Name : test
Number of users in the database : 3
==========================================================================
Local User Database Name : test123
Number of users in the database : 3
```

The following example displays the details of a particular user database. The passwords are encrypted in the example.

```
device#show local-userdb test
==========================================================================
Local User Database : test
Username           Password
--------           --------
user1              $e$&Z9'%*&+
user2              $e$,)A=)65N,%-3*%1?@U
user3              $e$5%&-5%YO&&A1%6%<@U
```

The following example displays details of a particular user in a specific database.

```
device# show local-userdb db1 user1
Username = user1  Password = $e$%U*V
```

show logging

Displays the Syslog messages in the device local buffer.

Syntax

show logging

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

All configuration modes

Command Output

The **show logging** command displays the following information:

Output field	Description
Syslog logging	The state (enabled or disabled) of the Syslog buffer.
messages dropped	The number of Syslog messages dropped due to user-configured filters. By default, the software logs messages for all Syslog levels. You can disable individual Syslog levels, in which case the software filters out messages at those levels. Each time the software filters out a Syslog message, this counter is incremented.
flushes	The number of times the Syslog buffer has been cleared by the clear logging command or equivalent Web Management Interface option.
overruns	The number of times the dynamic log buffer has filled up and been cleared to hold new entries. For example, if the buffer is set for 100 entries, the 101st entry causes an overrun. After that, the 201st entry causes a second overrun.
level	The message levels that are enabled. Each letter represents a message type and is identified by the key (level code) below the value. If you disable logging of a message level, the code for that level is not listed.
messages logged	The total number of messages that have been logged since the software was loaded.
level code	The message levels represented by the one-letter codes.

Examples

The following is a sample output of the **show logging** command.

```
device# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 24 overruns)
    Buffer logging: level ACDMEINW, 50 messages logged
    level code: A=alert C=critical D=debugging M=emergency E=error
                I=informational N=notification W=warning

Static Log Buffer:
Jan  1 00:00:47:I:System: Stack unit 1 PSU fan direction mismatch

Dynamic Log Buffer (50 lines):
Jan  3 20:23:10:I:Security: startup-config was changed by operator from console
Jan  3 20:17:25:I:Security: startup-config was changed by operator from console
Jan  3 19:50:43:I:MSTP: MST 1 Port 1/1/11:1  - Bridge TC Event
Jan  3 19:50:43:I:MSTP: MST 0 Port 1/1/11:1  - Bridge TC Event
Jan  3 19:49:29:I:System: Logical link on dynamic lag interface ethernet 1/1/9:3 is up.
Jan  3 19:49:29:I:System: Interface ethernet 1/1/9:3, state up
Jan  3 19:49:29:I:System: Logical link on dynamic lag interface ethernet 1/1/9:1 is up.
Jan  3 19:49:29:I:System: Interface ethernet 1/1/9:1, state up
Jan  3 19:49:29:I:MRP: Interface ethernet 1/1/9:1 of ring 51  Vlan 51, changing to forwarding
Jan  3 19:49:29:I:MSTP: MST 1 Port 1/1/11:1  - Bridge TC Event
Jan  3 19:49:29:I:MSTP: MST 1 Port 1/1/9:1  - Bridge TC Event
Jan  3 19:49:29:I:MSTP: MST 1 Port 1/1/9:1 - FORWARDING
Jan  3 19:49:29:I:MSTP: MST 1 Port 1/1/9:1 - LEARNING
Jan  3 19:49:29:I:MSTP: MST 0 Port 1/1/11:1  - Bridge TC Event
Jan  3 19:49:29:I:MSTP: MST 0 Port 1/1/9:1  - Bridge TC Event
Jan  3 19:49:29:I:MSTP: MST 0 Port 1/1/9:1 - FORWARDING
Jan  3 19:49:29:I:MSTP: MST 0 Port 1/1/9:1 - LEARNING
Jan  3 19:49:29:I:System: Logical link on dynamic lag interface ethernet 1/1/9:4 is up.
Jan  3 19:49:29:I:System: Interface ethernet 1/1/9:4, state up
Jan  3 19:49:29:I:System: Logical link on dynamic lag interface ethernet 1/1/9:2 is up.
Jan  3 19:49:29:I:System: Interface ethernet 1/1/9:2, state up
Jan  3 19:49:29:I:MRP: Interface ethernet 1/1/9:1 of ring 51  Vlan 51, changing to preforwarding
Jan  3 19:49:29:I:MSTP: MST 1 Port 1/1/9:1 - DISCARDING
Jan  3 19:49:29:I:MSTP: MST 0 Port 1/1/9:1 - DISCARDING
Jan  3 19:49:29:I:Trunk: Group (1/1/9:1, 1/1/9:2, 1/1/9:3, 1/1/9:4) created by 802.3ad link-aggregation
module.
Jan  3 19:49:12:I:System: Interface ethernet 1/1/9:2, state down
Jan  3 19:49:12:I:System: Logical link on dynamic lag interface ethernet 1/1/9:2 is down.
Jan  3 19:49:12:I:MRP: Interface ethernet 1/1/9:1 of ring 51  Vlan 51, changing to disabled
Jan  3 19:49:12:I:MSTP: MST 0 Port 1/1/9:1 - DISCARDING
Jan  3 19:49:12:I:MSTP: MST 1 Port 1/1/9:1 - DISCARDING
Jan  3 19:49:12:I:Trunk: Group (1/1/9:1, 1/1/9:2, 1/1/9:3, 1/1/9:4) removed by 802.3ad link-aggregation
module.
Jan  3 19:49:12:I:System: Interface ethernet 1/1/9:4, state down
Jan  3 19:49:12:I:System: Logical link on dynamic lag interface ethernet 1/1/9:4 is down.
Jan  3 19:49:12:I:System: Interface ethernet 1/1/9:1, state down
Jan  3 19:49:12:I:System: Logical link on dynamic lag interface ethernet 1/1/9:1 is down.
Jan  3 19:49:12:I:System: Interface ethernet 1/1/9:3, state down
Jan  3 19:49:12:I:System: Logical link on dynamic lag interface ethernet 1/1/9:3 is down.
```

show loop-detection resource

Displays the hardware and software resource information on loop detection.

Syntax

show loop-detection resource

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show loop-detection resource** command displays the following information:

Output field	Description
alloc	Memory allocated
in-use	Memory in use
qvail	Available memory
get-fail	The number of get requests that have failed
Limit	The maximum memory allocation
get-mem	The number of get-memory requests
size	The size
init	The number of requests initiated

Examples

The following is a sample output of the **show loop-detection resource** command.

```
device# show loop-detection resource

Vlans configured loop-detection use 1 HW MAC
Vlans not configured but use HW MAC: 1 10
                                    alloc    in-use     avail    get-fail    limit  get-mem
size     init
configuration pool        16          6             10          0                 3712
6               15          16
linklist pool                 16          10            6           0                 3712
10              16          16
```

show loop-detection status

Displays loop detection status.

Syntax

show loop-detection status

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following is a sample output of the **show loop-detection status** command. If a port is errdisabled in Strict mode, it shows "ERR-DISABLE by itself". If it is errdisabled due to its associated vlan, it shows "ERR-DISABLE by vlan <num>"

```
device# show loop-detection status

loop detection packets interval: 10 (unit 0.1 sec)
Number of err-disabled ports: 3
You can re-enable err-disable ports one by one by "disable" then "enable"
under interface config, re-enable all by "clear loop-detect", or
configure "errdisable recovery cause loop-detection" for automatic recovery

index     port/vlan     status                                #errdis    sent-pkts    recv-pkts
1            1/1/13           untag, LEARNING              0             0                    0
2            1/1/15           untag, BLOCKING              0             0                    0
3            1/1/17           untag, DISABLED              0             0                    0
4         1/1/18         ERR-DISABLE by itself     1             6                 1
5            1/1/19           ERR-DISABLE by vlan12     0                0                    0
6            vlan12     ERR-DISABLE ports         2             24                2
```

show loop-detect no-shutdown-status

Shows the status of interfaces in a loop.

Syntax

show loop-detect no-shutdown-status

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show loop-detect no-shutdown-status** command displays the following information:

Output field	Description
Port	The specific interface
Loop status	The duration the port has been in a loop

Examples

The following example shows the ports and their loop statuses.

```
device# show loop-detection no-shutdown-status

loop detection no shutdown syslog interval : 5     (unit 1 min /Default 5 min)
loop detection no shutdown port status     :
Note: Port's loop status gets cleared if loop is not detected in a particular interval window

                Port    ||  Loop Status
      ==================||=========================
       ethernet  1/1/7  ||  (In Loop For 2309 Seconds)
       ethernet  1/1/15 ||  (In Loop For 2309 Seconds
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-address

Displays the MAC address table.

Syntax

show mac-address [**ethernet** *stack/slot/port* | **vlan** *vlan-id*] [*mac-address* [*mac-address-mask*]]

show mac-address [**all** | **session** | **statistics** | **mdup-stats** | **mdb** [**source-rbridge** *source-rbridgeid* **client-rbridge** *client-rbridgeid*]]

Parameters

ethernet *stack/slot/port*
: Displays information for the specific Ethernet port.

vlan *vlan-id*
: Displays the MAC address for the specified VLAN ID.

mac-address
: Displays the information for the specified Ethernet MAC address.

mac-address-mask
: Displays the information for the specified Ethernet MAC address mask.

all
: Displays MAC address of all ports including the blocked ports.

session
: Displays the MAC address of the ports in the session.

statistics
: Displays the MAC address statistics.

mdup-stats
: Displays MAC database update statistics. This option is available only on FSX devices.

mdb
: Displays information about the MAC database used in a cluster configuration. This option is available only on FSX devices.

source-rbridge *source-rbridgeid*
: Specifies the source RBridge ID. This option is available only on FSX devices.

client-rbridge *client-rbridgeid*
: Specifies the client RBridge ID. This option is available only on FSX devices.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

Command Output

The **show mac-address** command displays the following information:

Output field	Description
MAC-Address	The MAC address.
Type	Indicates whether the MAC entry is static or dynamic. A static entry is one you create using the **static-mac-address** command. A dynamic entry is one that is learned by the software from network traffic.

Usage Guidelines

The **show mac-address** command output does not include MAC addresses for management ports, because these ports do not support typical MAC learning and MAC-based forwarding.

Examples

The following example displays sample output of the **show mac-address** command.

```
device# show mac-address
Total active entries from all ports = 3
Total static entries from all ports = 1
MAC-Address       Port        Type      VLAN
0000.0034.1234    1/1/15      Static    1
0000.0038.2f24    1/1/14      Dynamic   1
0000.0038.2f00    1/1/13      Dynamic   1
0000.0086.b159    1/1/10      Dynamic   1
```

The following example displays sample output of the **show mac-address** command for a VLAN.

```
device# show mac-address vlan 1 0000.0000.0001
Total active entries from all ports = 16
MAC-Address       Port     Type      Index
0000.0000.0001    1/1/1      Dynamic   NA
Present in following devices (at hw index) :-
0 (8196 )       4 (8196 )
```

show mac-address cluster

Displays all the MAC address entries for a cluster.

Syntax

show mac-address cluster { *cluster-name* | *cluster-id* } [**vlan** *vlan-id*] [**client** [*client-name* | *client-id*]] [**local** | **remote** [**exclude-interface** | **interface**]]

Parameters

cluster-name
Displays the details for the cluster with the specified cluster name.

cluster-id
Displays the details for the cluster with the specified cluster ID.

vlan *vlan-id*
Displays the details for the VLAN with the specified VLAN ID.

client
Displays the details for the configured client.

client-name
Displays the details for the configured client with the specified client name.

client-id
Displays the details for the configured client with the specified client ID.

local
Displays the cluster local MAC address.

remote
Displays the cluster remote MAC address.

exclude-interface
Displays the MAC address of the remote cluster excluding the interface MAC address of the remote cluster.

interface
Displays the cluster remote interface MAC address.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Cluster configuration mode

Usage Guidelines

The **exclude-interface** and **interface** keywords are available only with the **remote** option. They are not available when the **client** option or the **vlan** option is used. When the **vlan** option is used, you can specify only the client name and not the client ID.

Examples

The following example shows the output of the **show mac-address cluster** command.

```
device# show mac-address cluster 1000
Total Cluster Enabled(CL+CR+CCL+CCR) MACs: 1
Total Cluster Local(CL) MACs: 1
CCL: Cluster Client Local CCR:Cluster Client Remote CL:Local CR:Remote
Total active entries from all ports = 1
Total static entries from all ports = 3
MAC-Address       Port    Type     Index   MCT-Type   VLAN
0000.0022.3333    1/1/1   Static   4254    CML        20
0000.0022.3333    1/1/3   Static   4254    CML        20
0000.0022.3333    1/1/13  Static   4254    CML        20
```

show mac-address mdb

Displays information about the MAC database used in cluster configuration.

Syntax

show mac-address mdb [**source-rbridge** *rbridge-id* **client-rbridge** *client-rbridge-id*]

Parameters

source-rbridge *rbridge-id*

Displays information about MAC database corresponding to a particular source RBridge. The range is from 1 to 4095.

client-rbridge *client-rbridge-id*

Displays information about MAC database corresponding to a particular client RBridge. The range is from 1 to 4095.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

.

show mac-authentication configuration

Displays the global or interface level MAC authentication configuration.

Syntax

show mac-authentication configuration [**all** | **ethernet** *device/slot/port*]

Parameters

all

Displays the MAC authentication configuration on all interfaces.

ethernet *device/slot/port*

Displays the MAC authentication configuration for a specific interface.

Modes

EXEC or Privileged EXEC mode

Global configuration mode

Usage Guidelines

Command Output

The **show mac-authentication configuration** command displays the following information.

Output field	Description
Status	Displays if MAC authentication is enabled or disabled
Auth-order	The authentication order enabled on the device
Default VLAN	The default VLAN specified on the device
Restricted VLAN	The restricted VLAN specified on the device
Critical VLAN	The critical VLAN specified on the device
Action on Auth failure	The action to be taken on authentication failure
MAC Session Aging	The status of the MAC session aging
Filter Strict Security	The status of filter strict security
Re-authentication	The status of re-authentication
Dot1x Override	The status of dot1x override
Password Override	The status of password override
Password Format	The configured password format
Reauth-period	The re-authentication period specified in seconds
Session max sw-age	The maximum software age configured on the device
Session max hw-age	The maximum hardware age configured on the device

The **show mac-authentication configuration all** | **ethernet***device/slot/port* command displays the following information.

Output field	Description
Auth Order	Displays the authentication order
Action on Auth failure	Displays the action to be taken on authentication failure
Action on Auth timeout	Displays the action to be taken on authentication timeout
Filter Strict Security	Displays if filter strict security is enabled or disabled
DoS Protection	Displays if DoS protection is enabled or disabled
Source-guard Protection	Displays if Source-Guard Protection is enabled or disabled
Aging	Displays if aging is enabled or disabled
Max-sessions	Displays the count of the maximum sessions
Ingress-filtering	Displays if ingress filtering is enabled or disabled

Examples

The following example displays the system level MAC authentication configuration.

```
device# show mac-authentication configuration

Status : Enabled
Auth Order : dot1x mac-auth
Default VLAN : 4
Restricted VLAN : Not configured
Critical VLAN : Not configured
Action on Auth failure : Block traffic
MAC Session Aging : Enabled
Filter Strict Security : Enabled
Re-authentication : Enabled
Dot1x Override : Disabled
Password Override : Disabled
Password Format : xxxx.xxxx.xxxx
Reauth-period : 600 seconds
Session max sw-age : 120 seconds
Session max hw-age : 70 seconds
```

The following example displays the MAC authentication configuration for port 1/1/15.

```
device# configure terminal
device(config)# show mac-authentication configuration 1/1/15

Port 1/1/15 Configuration:
Auth Order                      : dot1x mac-auth
Action on Auth failure          : Block traffic
Action on Auth timeout          : Treat as a failed authentication
Filter Strict Security          : Enabled
DoS Protection                  : Disabled (limit = 512)
Source-guard Protection         : Disabled
Aging                           : Enabled
Max-sessions                    : 32
Auth Filter List (Filter/VLAN) : 1/2
```

The following example displays the MAC authentication information on all interfaces.

```
device# configure terminal
device(config)# show mac-authentication configuration all

Port 1/1/1 Configuration:
Auth Order                      : dot1x mac-auth
Action on Auth failure          : Block traffic
Action on Auth timeout          : Treat as a failed authentication
Filter Strict Security          : Enabled
DoS Protection                  : Disabled (limit = 512)
Source-guard Protection         : Disabled
Reauth-timeout                  : 60 seconds
Aging                           : Enabled
Max-sessions                    : 2

Port 1/1/3 Configuration:
Auth Order                      : dot1x mac-auth
Action on Auth failure          : Block traffic
Action on Auth timeout          : Treat as a failed authentication
Filter Strict Security          : Enabled
DoS Protection                  : Disabled (limit = 512)
Source-guard Protection         : Disabled
Reauth-timeout                  : 60 seconds
Aging                           : Enabled
Max-sessions                    : 2
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-authentication ip-acl

Shows the layer 3 access lists (ACLs) for MAC authentication.

Syntax

show mac-authentication ip-acl { **all** | **ethernet** *device/slot/port* }

Parameters

all

Specifies the ACLs at the global level.

ethernet *device/slot/port*

Specifies the ACLs at the interface level.

Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

Examples

The **show mac-authentication ip-acl** command displays the following information.

```
device(config)# show mac-authentication ip-acl all
MAC-Auth IP ACL Information :

Port 1/1/15 : 0010.9400.0010
In-bound IP ACL : 101

Port 1/1/15 : 0010.9400.0020
In-bound IP ACL : 101

Port 2/1/15 : 0015.9400.0020
In-bound IP ACL : 102

device(config)# show mac-auth ip-acl eth 1/1/15
MAC-Auth IP ACL Information :

Port 1/1/15 : 0010.9400.0010
In-bound IP ACL : 101

Port 1/1/15 : 0010.9400.0020
In-bound IP ACL : 101
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-authentication sessions

Shows MAC authentication sessions at a global and interface level.

Syntax

show mac-authentication sessions { **all** | **brief** | **ethernet** *unit/slot/port* }

Parameters

all

Specifies the MAC authentication sessions for all ports.

brief

Specifies details of MAC authentication sessions in brief.

ethernet *unit/slot/port*

Specifies the MAC authentication sessions of an interface.

Modes

Privileged EXEC mode

Global configuration

Interface configuration

Authentication configuration mode

Command Output

The **show mac-authentication sessions** command displays the following information:

Output field	Description
Port	The port number.
MAC Address	The MAC address of the client.
IP Address	The IP address of the client. The IP address of the authenticated host is displayed only if an IP ACL is applied to the interface based on the RADIUS server response.
VLAN	The VLAN
Auth State	The authentication state.
ACL	The specific ACL applied.
Age	The age of the session.

Examples

The following example displays MAC authentication sessions for all interfaces.

```
device# show mac-authentication sessions all
--------------------------------------------------------------------------------
Port        MAC              IP              Vlan  Auth      ACL     Age
            Addr             Addr                  State
--------------------------------------------------------------------------------
1/1/2       0010.94ab.0021   N/A             300   Yes       none       Ena
```

The following example displays MAC authentication sessions for a specified interface.

```
device# show mac-authentication sessions ethernet 1/1/2
--------------------------------------------------------------------------------
Port        MAC              IP              Vlan  Auth      ACL     Age
            Addr             Addr                  State
--------------------------------------------------------------------------------
1/1/2       0010.94ab.0021   N/A             300   Yes       none       Ena
```

The following example displays MAC authentication sessions brief.

```
device# show mac-authentication sessions brief
------------------------------------------------------------------------------------------------
Port      Number of           Number of          Number of         Untagged         Dynamic
          Attempted Users     Authorized Users   Denied Users      VLAN Type        Port ACL
------------------------------------------------------------------------------------------------
1/1/2     1                   1                  0                 Radius-VLAN         No
1/1/3     0                   0                  0                 Auth-Default-VLAN   No
1/1/4     0                   0                  0                 Auth-Default-VLAN   No
1/1/5     0                   0                  0                 Auth-Default-VLAN   No
2/1/1     0                   0                  0                 Auth-Default-VLAN   No
2/1/2     0                   0                  0                 Auth-Default-VLAN   No
2/1/4     0                   0                  0                 Auth-Default-VLAN   No
```

History

Release version	Command history
08.0.20	This command was introduced.

show mac-authentication statistics

Displays the MAC authentication statistics.

Syntax

show mac-authentication statistics { **all** | **ethernet** *device/slot/port* }

Parameters

all

Displays the MAC authentication statistics for all interfaces.

ethernet *device/slot/port*

Displays the MAC authentication statistics for the specified interface.

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The **show mac-authentication statistics** command displays the following information:

Output field	Description
Accepted Sessions	The number of accepted sessions
Rejected Sessions	The number of rejected sessions
Inprogress Sessions	The number of in-progress sessions
Attempted Sessions	The number of attempted sessions
Number of Errors	The number of errors

Examples

The following example displays MAC authentication statistics for all interfaces.

```
device# show mac-authentication statistics all

Port 1/1/15 Statistics:
Accepted Sessions       :    2
Rejected Sessions       :    0
Inprogress Sessions     :    0
Attempted Sessions      :    0
Number of Errors        :    0

Port 2/1/15 Statistics:
Accepted Sessions       :    1
Rejected Sessions       :    0
Inprogress Sessions     :    0
Attempted Sessions      :    0
Number of Errors        :    0
```

The following example displays MAC authentication statistics for Ethernet interface 1/1/15.

```
device# show mac-auth statistics ethernet 1/1/15

Port 1/1/15 Statistics:
Accepted Sessions       :    2
Rejected Sessions       :    0
Inprogress Sessions     :    0
Attempted Sessions      :    0
Number of Errors        :    0
```

History

Release version	Command history
08.0.20	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 *device/slot/port*

Parameters

device/slot/port

Interface for which MACsec status information is to be displayed. The interface is designated by device number in stack/slot on the device/interface on the slot.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

dot1x-mka configuration mode

dot1x-mka-interface configuration mode

Usage Guidelines

This command is supported only on the Brocade ICX 6610 in FastIron Release 08.0.20. In FastIron Release 08.0.30 and later releases, MACsec commands are also supported on the ICX 7450.

It is recommended that you use the **clear macsec ethernet** command to clear previous results for the **show macsec statistics ethernet** command before re-executing it.

Command Output

The **show macsec statistics ethernet** command displays the following information:

Output field	Description
Interface (Device/slot/port)	The information that follows describes the designated interface.
Replay Protection (Enabled, Disabled)	Indicates whether replay protection is applied on the interface.
Replay Window (0 through 127)	If out-of-order packets are allowed, indicates allowable window within which an out-of-order packet can be received.
Frame Validation (Enabled, Disabled)	Indicates whether MACsec frame headers are checked.
Secure Channel Statistics:	The fields that follow describe activity on a secure channel established over the designated interface.
TxPktProtectedOnly	Number of transmitted packets with integrity protection only.
TxOctetProtectedOnly	Number of bytes transmitted in packets with integrity protection only.
TxPktEncrypted	Number of transmitted packets that are encrypted.
TxOctetEncrypted	Number of bytes transmitted in encrypted packets.

Output field	Description
TxPktMiss	Number of transmitted packets that are neither encrypted nor protected by integrity check.
TxOctetMiss	Number of bytes transmitted in packets that are neither encrypted nor protected by integrity checking.
TxPktDrop	Number of packets dropped at transmission because SAK has been exhausted.
TxPktBad	Number of transmitted packets marked as bad.
RxPktDecryptedAuth	Number of packets received, decrypted, and checked for integrity protection.
RxOctetTotal	Number of bytes received.
RxOctetAuthOnly	Number of bytes received with Integrity protection only.
RxOctetDecrypted	Number of bytes received and decrypted.
RxPktFailReplayCheck	Number of packets received out of order.
RxPktFailICVCheck	Number of packets received that failed Integrity checking.
RxPktNoMACsecTag	Number of packets received without a MACSec Tag.
RxPktFrameValFail	Number of packets received that failed MACsec frame validation.
RxPktMiss	Number of packets received that did not find a key for decryption.
RxOctetMiss	Number of bytes received that did not find a key for decryption.
RxPktDrop	Number of received packets that were dropped.

Examples

The following example shows details for Ethernet interface 1/3/1 (device 1, slot 3, port 1). The interface is verifying MACsec frames and is providing strict replay protection. Based on counter statistics, transmitted packets are being encrypted. A smaller number of packets have been received, have passed integrity checking, and have been decrypted. No packets have been received out of order, and no packets have been dropped. No packets have failed integrity checking. A number of packets have been received without MACsec headers, and numerous bytes did not have a decryption key.

```
device(config-dot1x-mka-1/3/1)# clear macsec ethernet 1/3/1
device(config-dot1x-mka-1/3/1)# show macsec statistics ethernet 1/3/1

Interface                : 1/3/1

Replay Protection   : Enabled
Replay Window       : 0
Frame Validation    : Check

Secure Channel Statistics:
     TxPktProtectedOnly     165074761   TxOctetProtectedOnly          20491766144
         TxPktEncrypted             0       TxOctetEncrypted                    0
              TxPktMiss             0            TxOctetMiss                    0
              TxPktDrop             0               TxPktBad                    0

     RxPktDecryptedAuth          3455          RxOctetTotal                257506
        RxOctetAuthOnly        230740       RxOctetDecrypted                    0
   RxPktFailReplayCheck             0      RxPktFailICVCheck                    0
       RxPktNoMACsecTag           414      RxPktFrameValFail                    0
              RxPktMiss           414            RxOctetMiss                26766
              RxPktDrop             0
```

The following example shows output for an ICX 7450 device. The output for the ICX 7450 is different from the output for other devices.

```
device(config)#
device(config)#sh macsec stat ethe 10/2/1
device(config)#
Interface Statistics:
---------------------
rx Untag Pkts             : 1                   tx Untag Pkts             : 0
rx Notag Pkts             : 0                   tx TooLong Pkts           : 0
rx Badtag Pkts            : 0
rx Unknownsci Pkts        : 0
rx Nosci Pkts             : 0
rx Overrun Pkts           : 0

Transmit Secure Channels:
-------------------------

SA[0] Statistics:
Protected Pkts            : 0
Encrypted Pkts            : 2436337

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

SC Statistics:
Protected Octets          : 0                   Encrypted Octets          : 134830107
Protected Pkts            : 0                   Encrypted Pkts            : 2436337

Receive Secure Channels:
------------------------

SA[0] Statistics:
Ok Pkts                   : 1949642             Invalid Pkts              : 0
Not using SA Pkts         : 0                   Unused Pkts               : 0
Not Valid Pkts            : 0

SA[1] Statistics:
Ok Pkts                   : 0                   Invalid Pkts              : 0
Not using SA Pkts         : 0                   Unused Pkts               : 0
Not Valid Pkts            : 0

SA[2] Statistics:
Ok Pkts                   : 0                   Invalid Pkts              : 0
Not using SA Pkts         : 0                   Unused Pkts               : 0
Not Valid Pkts            : 0

SA[3] Statistics:
Ok Pkts                   : 0                   Invalid Pkts              : 0
Not using SA Pkts         : 0                   Unused Pkts               : 0
Not Valid Pkts            : 0

SC Statistics:
OkPkts                    : 1949642             Invalid Pkts              : 0
Not using SA Pkts         : 0                   Unused Pkts               : 0
Not Valid Pkts            : 0                   Unchecked Pkts            : 0
Delayed Pkts              : 0                   Late Pkts                 : 0
Valid Octets              : 0                   Decrypted Octets          : 97743896
device(config)#
```

History

Release version	Command history
08.0.20	This command was introduced.
08.0.20a	This command was modified. The **show macsec ethernet** command name was changed to **show macsec statistics ethernet**.

show management-vrf

Displays packet and session rejection statistics due to failure in management VRF validation.

Syntax

show management-vrf

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

Make sure that the management VRF is configured before executing the **show management-vrf** command.

Command Output

The **show management-vrf** command displays the following information:

Output field	Description
Management VRF name	Displays the configured management VRF name.
Management Application	Displays the management application names.
Rx Drop Pkts	Displays the number of packets dropped in the inbound traffic.
Tx Drop Pkts	Displays the number of packets dropped in the outbound traffic.
TCP Connection rejects	Displays the number of TCP connections per application rejected due to management VRF validation.

Examples

The following is a sample output of the **show management-vrf** command.

```
device(config)# show management-vrf

Management VRF name : sflow
Management Application     Rx Drop Pkts     Tx Drop Pkts
SNMP Engine
0                                             11
RADIUS Client
0                                                  0
TFTP Client
0                                                  0
Traps
-                                                  0
SysLogs
-                                                  0
TCP Connection rejects:
Telnet               : 0
SSH (Strict)     : 685
TACACS+ Client   : 0
```

show media

Displays information about the media devices installed per device, per stack, and per port.

Syntax

show media [**validation**] [**ethernet** *stackid/slot/port* | **stack** *stack-id*]

Parameters

validation

Displays whether the connected optic modules are supported or not on Brocade devices.

ethernet *stackid/slot/port*

Displays the media type for the specified Ethernet interface.

stack *stack-id*

Displays the media type for the specified stack.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show flash** command displays the Type, Vendor, Part number, Version and Serial number of the SFP, SFP+, or XFP optical device installed in the port. If there is no SFP, SFP+, or XFP optical device installed in a port, the "Type" field will display "EMPTY".

Examples

The following example is a sample output of the **show media** command. The **show media** command displays information about the media devices installed in a device.

```
device# show media

Port 1/1/1:        Type : 1G M-C (Gig-Copper)
Port 1/1/2:     Type : 1G M-C (Gig-Copper)
Port 1/1/3:     Type : 1G M-C (Gig-Copper)
Port 1/1/4:     Type : 1G M-C (Gig-Copper)
Port 1/1/5:     Type : 1G M-C (Gig-Copper)
Port 1/1/6:     Type : 1G M-C (Gig-Copper)
Port 1/1/7:     Type : 1G M-C (Gig-Copper)
Port 1/1/8:     Type : 1G M-C (Gig-Copper)
Port 1/1/9:     Type : 1G M-C (Gig-Copper)
Port 1/1/10:     Type : 1G M-C (Gig-Copper)
Port 1/1/11:     Type : 1G M-C (Gig-Copper)
Port 1/1/12:     Type : 1G M-C (Gig-Copper)
Port 1/1/13:     Type : 1G M-C (Gig-Copper)
Port 1/1/14:     Type : 1G M-C (Gig-Copper)
Port 1/1/15:     Type : 1G M-C (Gig-Copper)
Port 1/1/16:     Type : 1G M-C (Gig-Copper)
Port 1/1/17:     Type : 1G M-C (Gig-Copper)
Port 1/1/18:     Type : 1G M-C (Gig-Copper)
Port 1/1/19:     Type : 1G M-C (Gig-Copper)
Port 1/1/20:     Type : 1G M-C (Gig-Copper)
Port 1/1/21:     Type : 1G M-C (Gig-Copper)
Port 1/1/22:     Type : 1G M-C (Gig-Copper)
Port 1/1/23:     Type : 1G M-C (Gig-Copper)
Port 1/1/24:     Type : 1G M-C (Gig-Copper)
Port 1/2/1:     Type : 10GE SR 300m (SFP +)
Port 1/2/2:     Type : EMPTY
Port 1/2/3:     Type : 1G Twinax 1m (SFP)
Port 1/2/4:     Type : 1G Twinax 1m (SFP)
```

The following is a sample output of the **show media validation** command. The output displays whether the connected optic modules are supported or not on Brocade devices.

```
device# show media validation

Port       Supported Vendor               Type
-----------------------------------------------------------------------
1/1/9:1    Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/1/9:2    Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/1/9:3    Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/1/9:4    Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/1/11:1   Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/1/11:2   Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/1/11:3   Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/1/11:4   Yes       BROCADE               Type  : 4x10GE Active Copper 1m (QSFP+)
1/3/1      Yes       BROCADE               Type  : 40GE-SR4 100m (QSFP+)
```

The following is a sample output of the **show media stack**command.

```
device# show media stack 1

Port 1/1/1:  Type  : EMPTY
Port 1/1/2:  Type  : EMPTY
Port 1/1/3:  Type  : EMPTY
Port 1/1/4:  Type  : EMPTY
Port 1/1/5:  Type  : EMPTY
Port 1/1/6:  Type  : EMPTY
Port 1/1/7:  Type  : EMPTY
Port 1/1/8:  Type  : EMPTY
Port 1/1/9:1:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/9:2:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/9:3:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/9:4:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/10:  Type  : EMPTY
Port 1/1/11:1:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/11:2:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/11:3:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/11:4:  Type  : 4x10GE Active Copper 1m (QSFP+)
Port 1/1/12:  Type  : EMPTY
Port 1/1/13:  Type  : EMPTY
Port 1/1/14:  Type  : EMPTY
Port 1/1/15:  Type  : EMPTY
Port 1/1/16:  Type  : EMPTY
Port 1/1/17:  Type  : EMPTY
Port 1/1/18:  Type  : EMPTY
Port 1/1/19:  Type  : EMPTY
Port 1/1/20:  Type  : EMPTY
Port 1/2/1:  Type  : EMPTY
Port 1/2/2:  Type  : EMPTY
Port 1/2/3:  Type  : EMPTY
Port 1/2/4:  Type  : EMPTY
Port 1/2/5:  Type  : EMPTY
Port 1/2/6:  Type  : EMPTY
Port 1/3/1:  Type  : 40GE-SR4 100m (QSFP+)
Port 1/3/2:  Type  : EMPTY
Port 1/3/3:  Type  : EMPTY
Port 1/3/4:  Type  : EMPTY
Port 1/3/5:  Type  : EMPTY
Port 1/3/6:  Type  : EMPTY
```

The following is a sample output of the **show media ethernet** command.

```
device# show media ethernet 1/3/1
Port    1/3/1: Type  : 40GE-SR4 100m (QSFP+)
            Vendor: BROCADE           Version: A
            Part# : 57-1000128-01     Serial#: LTA112251000543
```

show memory

Displays the memory usage for system tasks, transmission control protocol, and stack units.

Syntax

show memory [**task** | **tcp** | **unit** *unit-id*]

Parameters

task

Displays memory usage per system task.

tcp

Displays Transmission Control Protocol (TCP) memory usage.

unit *unit-id*

The ID of the stack unit.

Modes

Global configuration mode

User EXEC mode

Usage Guidelines

Command Output

The **show memory task** command displays the following information:

Output field	Description
Task	The name of the task.
Alloc	The amount memory allocated for the task.
Free	The amount of free memory available.
Used	The amount of memory used by the specific task.
TCB usage	The availability of Transmission Control Block for the TCP connection.
TCP QUEUE BUFFER usage	The availability of the Queue buffer used to hold the TCP messages that need to be sent.
TCP SEND BUFFER usage	The availability of buffers which will be used to send the TCP packets from the device.
TCP RECEIVE BUFFER usage	The availability of buffers which will be used to receive the TCP packets to the device.
TCP OUT OF SEQUENCE BUFFER usage	The availability of re-sequence buffer used for the TCP connection.

Examples

The following example command displays the memory usage per task.

```
Task Memory Usage Info
------------------------------
Last clear : NA
----------------------------------------------------------------------
Task                          Alloc         Free          Used
----------------------------------------------------------------------
TimerTsk                        144            0           144
FlashTsk                       5552            0          5552
MainTsk                    33153780      3411177      29742603
keygen                        1468            0          1468
itc                           9188            0          9188
bcmCNTR.0                    17820            0         17820
bcmL2MOD.0                     144            0           144
scp                         232815        27166        205649
appl                      676257682    637313495      38944187
snms                         127713        52104         75609
rtm                         9476869        17272       9459597
rtm6                         321341        17272        304069
rip                          574422         8636        565786
bgp                         4048555        17272       4031283
ospf                        2937465         8636       2928829
openflow_ofm                 431242        14621        416621
openflow_opm                 433909        17272        416637
mcast_fwd                   1776859        17272       1759587
mcast                       2614790        31233       2583557
msdp                         221375        17272        204103
ripng                         96181         8636         87545
ospf6                       1989857         8636       1981221
mcast6                       794175        22597        771578
ipsec                        208381         8636        199745
dhcp6                        134907         8636        126271
snmp                          57140        17272         39868
rmon                          74775        17272         57503
web                           56915        17344         39571
acl                         1291591        28243       1263348
flexauth                     277607         8636        268971
ntp                           56835        17272         39563
rconsole                      48215         8636         39579
console                     2059410      1476779        582631
ospf_msg_task                 56035        17272         38763
auxTsk                         4572            0          4572
bcmLINK.0                     37152        37152             0
Total Memory Used: 97213162
```

The following example displays the TCP memory usage information.

```
device# show memory tcp
TCP MEMORY USAGE
TCB usage: total=73140, free=71300
TCP QUEUE BUFFER usage: total=19635, free=19635
TCP SEND BUFFER usage: total=192532, free=192532
TCP RECEIVE BUFFER usage: total=192532, free=192532
TCP OUT OF SEQUENCE BUFFER usage: total=25074, free=25074
```

The following example displays memory usage for stack unit 1.

```
device# show memory unit 1
Stack unit 1:
  Total DRAM: 268435456 bytes
  Dynamic memory: 3781353472 bytes total, 3563307008 bytes free, 5% used
```

History

Release version	Command history
08.0.30	This command was introduced.

show memory task

Displays the memory usage, allocated memory, and free memory for system tasks on the device.

Syntax

show memory task [**clear**]

Parameters

clear

Clears the displayed memory information if no memory is used.

Modes

Global configuration mode

User EXEC mode

Usage Guidelines

Examples

The following example displays the memory usage, allocated memory, and free memory for system tasks on the device.

```
device# show memory task
Task Memory Usage Info
----------------------
Last clear : NA
----------------------------------------------------------------------
 Task                          Alloc         Free        Used
----------------------------------------------------------------------
TimerTsk                         144            0         144
FlashTsk                        5552            0        5552
MainTsk                     33153780      3411177    29742603
keygen                         1468            0        1468
itc                            9188            0        9188
bcmCNTR.0                     17820            0       17820
bcmL2MOD.0                      144            0         144
scp                          232815        27166      205649
appl                      676257682    637313495    38944187
snms                         127713        52104       75609
rtm                         9476869        17272     9459597
rtm6                         321341        17272      304069
rip                          574422         8636      565786
bgp                         4048555        17272     4031283
ospf                        2937465         8636     2928829
openflow_ofm                 431242        14621      416621
openflow_opm                 433909        17272      416637
mcast_fwd                   1776859        17272     1759587
mcast                       2614790        31233     2583557
msdp                         221375        17272      204103
ripng                         96181         8636       87545
ospf6                       1989857         8636     1981221
mcast6                       794175        22597      771578
ipsec                        208381         8636      199745
dhcp6                        134907         8636      126271
snmp                          57140        17272       39868
rmon                          74775        17272       57503
web                           56915        17344       39571
acl                         1291591        28243     1263348
flexauth                     277607         8636      268971
ntp                           56835        17272       39563
rconsole                      48215         8636       39579
console                     2059410      1476779      582631
ospf_msg_task                 56035        17272       38763
auxTsk                         4572            0        4572
bcmLINK.0                     37152        37152           0
Total Memory Used: 97213162
```

History

Release version	Command history
08.0.30	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 mirror

Displays the port mirroring configuration details.

Syntax

show mirror ethernet *stackid/slot/port*

Parameters

ethernet *stackid/slot/port*

Displays the details for the specified Ethernet port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Examples

The following example displays sample output of the **show mirror** command.

```
device(config)# show mirror ethernet 1/2/1
Mirror port 1/2/1
  Input monitoring      : (U1/M1)   2
  Output monitoring     : None
```

show monitor

Displays the monitored ports configurations.

Syntax

show monitor ethernet *stackid/slot/port*

Parameters

ethernet *stackid/slot/port*

Displays the information for the specified monitored Ethernet port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example displays sample output of the **show monitor** command.

```
device> show monitor ethernet 1/1/2
  Input mirrored by     : (U1/M2)   1
  Output mirrored by    : None
```

show module

Displays module information for stack members.

Syntax

show module

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

Command Output

The **show module** command displays the following information:

Output field	Description
Module	Identifies the module by stack unit ID, module number, and module type.
Status	The status of this module.
Ports	The number of ports in this module.
Starting MAC	The starting MAC address for this module.

Examples

The following example displays stack module information.

```
device# show module

       Module                                        Status  Ports Starting MAC
U1:M1  ICX7450-48 48-port Management Module            OK      48   cc4e.248d.f8d0
U1:M2  ICX7400-4X10GF 4-port 40G Module               OK      4    cc4e.248d.f901
U1:M3  ICX7400-1X40GQ 1-port 40G Module               OK      1    cc4e.248d.f905
U2:M1  ICX7450-48 48-port Management Module            OK      48   cc4e.248e.4990
U2:M2  ICX7400-4X10GF 4-port 40G Module               OK      4    cc4e.248e.49c1
U2:M3  ICX7400-SERVICE-MOD Module                     OK      0
U2:M4  ICX7400-1X40GQ 1-port 40G Module               OK      1    cc4e.248e.49c9
U3:M1  ICX7450-48 48-port Management Module            OK      48   cc4e.248e.4490
U3:M2  ICX7400-4X10GF 4-port 40G Module               OK      4    cc4e.248e.44c1
U3:M3  ICX7400-1X40GQ 1-port 40G Module               OK      1    cc4e.248e.44c5
U3:M4  ICX7400-1X40GQ 1-port 40G Module               OK      1    cc4e.248e.44c9
```

The following example displays stack module information when a module is removed form the device.

```
device#show module
        Module                                              Status Ports Starting MAC
U1:M1  ICX7450-24P POE 24-port Management Module       OK     24   cc4e.248e.5648
U1:M2  ICX7400-4X10GF 4-port 40G Module               CFG     4   cc4e.248e.5665
U1:M3  ICX7400-1X40GQ 1-port 40G Module               OK      1   cc4e.248e.5665
U1:M4  ICX7400-1X40GQ 1-port 40G Module               OK      1   cc4e.248e.5669
device#
```

show mstp

Displays the MSTP information.

Syntax

show mstp { [**detail**] *mstp-id* | **configuration** }

Parameters

detail

Displays detailed MSTP information for the specified ID.

mstp-id

Displays the MSTP information for a specific ID.

configuration

Displays MSTP configuration information.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

Command Output

The **show mstp** command displays the following information:

Output field	Description
MSTP Instance	The ID of the MSTP instance whose statistics are being displayed. For the CIST, this number is 0.
VLANs	The number of VLANs that are included in this instance of MSTP. For the CIST, this number will always be 1.
Bridge Identifier	The MAC address of the bridge.
Bridge MaxAge sec	Displays the configured maximum age.
Bridge Hello sec	Displays the configured Hello variable.
Bridge FwdDly sec	Displays the configured FwdDly variable.
Bridge Hop cnt	Displays the configured Max Hop count variable.
Root MaxAge sec	The maximum age configured on the root bridge.
Root Hello sec	Hello interval configured on the root bridge.
Root FwdDly sec	FwdDly interval configured on the root bridge.
Root Hop Cnt	Maximum hop count left from the root bridge.
Root Bridge	Bridge identifier of the root bridge.

Output field	Description
ExtPath Cost	The configured path cost on a link connected to this port to an external MSTP region.
Regional Root Bridge	The Regional Root Bridge is the MAC address of the root bridge for the local region.
IntPath Cost	The configured path cost on a link connected to this port within the internal MSTP region.
Designated Bridge	The MAC address of the bridge that sent the best BPDU that was received on this port.
Root Port	Port indicating shortest path to root. Set to "Root" if this bridge is the root bridge.
Port Num	The port number of the interface.
Pri	The configured priority of the port. The default is 128.
PortPath Cost	Configured or auto-detected path cost for port.
P2P Mac	Indicates if the port is configured with a point-to-point link: • T - The port is configured in a point-to-point link. • F - The port is not configured in a point-to-point link.
Edge	Indicates if the port is configured as an operational edge port: • T - Indicates that the port is defined as an edge port. • F - Indicates that the port is not defined as an edge port.
Role	The port current spanning tree state. A port can have one of the following states: • Forwarding • Discarding • Learning • Disabled
Designated Cost	Port path cost to the root bridge.
Max Hop cnt	The maximum hop count configured for this instance.

Examples

The following example displays the MSTP information for a specified MSTP instance.

```
device# show mstp 1
MSTP Instance 1 - VLANs: 2
-------------------------------------------------------------------------------
Bridge            Max          RegionalRoot       IntPath     Designated       Root    Root
Identifier        Hop          Bridge             Cost        Bridge           Port    Hop
hex               cnt          hex                            hex                      cnt
8001000cdb80af01  20           8001000cdb80af01   0           8001000cdb80af01  Root   20
Port    Pri       PortPath     Role State         Designa-    Designated
Num     Cost                                     ted cost    bridge
3/1 128 2000      MASTER       FORWARDING         0           8001000cdb80af01
```

The following example displays the detailed MSTP information.

```
device# show mstp detail
MSTP Instance 0 (CIST) - VLANs: 4093
-------------------------------------------------------------------------
Bridge: 800000b000c00000 [Priority 32768, SysId 0, Mac 00b000c00000]
FwdDelay 15, HelloTime 2, MaxHops 20, TxHoldCount 6
Port 6/54 - Role: DESIGNATED - State: FORWARDING
PathCost 20000, Priority 128, OperEdge T, OperPt2PtMac F, Boundary T
Designated - Root 800000b000c00000, RegionalRoot 800000b000c00000,
Bridge 800000b000c00000, ExtCost 0, IntCost 0
ActiveTimers - helloWhen 1
MachineState - PRX-DISCARD, PTX-IDLE, PPM-SENDING_RSTP, PIM-CURRENT
PRT-ACTIVE_PORT, PST-FORWARDING, TCM-INACTIVE
BPDUs - Rcvd MST 0, RST 0, Config 0, TCN 0
Sent MST 6, RST 0, Config 0, TCN 0
```

The following example displays the MSTP configuration details.

```
device# show mstp configuration
MSTP CONFIGURATION
------------------
Name : Reg1
Revision : 1
Version : 3 (MSTP mode)
Status : Started
Instanc  VLANs
-------- --------------
0        4093
```

show notification-mac

Displays whether MAC-notification for SNMP traps is enabled or disabled.

Syntax

show notification-mac

Modes

Privileged EXEC mode

Usage Guidelines

You can view statistics such as the configured interval, the number of traps sent, and the number of events sent.

Examples

The following example displays the MAC-notification statistics:

```
device# show notification-mac
Mac-notification SNMP trap is ENABLED
Configured Interval: 40 seconds
Number of trap messages sent: 2
Number of mac-notification events sent: 20
```

History

Release version	Command history
08.0.10	This command was introduced.

show notification mac-movement

Displays the MAC address movement notifications.

Syntax

show notification mac-movement { **interval-history** | **threshold-rate** }

Parameters

interval-history

Displays the collected history of MAC address movement notification and how the history interval is configured.

threshold-rate

Displays the configuration of the MAC address movement threshold rate.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show notification mac-movement interval-history** command displays the following information:

Output field	Description
Interval-History Mac Movement Notification	Specifies whether the interval history data collection is enabled.
Configured Interval	The interval over which the MAC address movement statistics were collected.
Number of macs that moved in the interval	The number of MAC addresses that moved during the configured interval regardless of how many times each address moved.
Total number of moves in the interval	The total number of MAC address moves over the configured interval.
Interval Move-Count	The number of times the MAC address has moved within the interval.

The **show notification mac-movement threshold-rate** command displays the following information:

Output field	Description
Threshold-Rate Mac Movement Notification	Specifies whether the MAC movement notification threshold rate is enabled.
Configured Threshold-Rate	The rate in MAC address moves per sampling interval after which a notification is issued. The range is from 1 through 50000.
Configured Sampling-Interval	The sampling interval in seconds over which the number of MAC address moves is measured. The range is from 1 through 86400, which is the number of seconds in a day.
Number of entries in the notification table	One entry for each time a MAC address notification threshold was reached.
MAC-Address	The MAC address that has moved to a different port.
from-Port	The port from which the MAC address moved.

Output field	Description
to-Port	The port to which the MAC address moved.
Last Move-Time	The time the last move occurred. The system uptime is used if there is no time server configured.
Vlan-id	The VLAN for the port where the MAC address movement was detected.

Examples

The following example displays the notification interval history.

```
device# show notification mac-movement interval-history
Interval-History Mac Movement Notification is ENABLED
Configured Interval : 30 seconds
Number of macs that moved in the interval : 100
Total number of moves in the interval : 98654
MAC-Address       from-Port   to-Port   Interval Move-Count   Last Move-Time   Vlan-id
--------------    ---------   -------   -------------------   --------------   -------

0000.0000.0052    7/1         7/2        1000                 May 15 01:13:20   10
0000.0000.0051    7/1         7/2        1002                 May 15 01:13:20   10
0000.0000.0050    7/1         7/2        1012                 May 15 01:13:20   10
0000.0000.004f    7/1         7/2        1018                 May 15 01:13:20   10
0000.0000.004e    7/1         7/2        1012                 May 15 01:13:20   10
(output truncated)
```

The following examples displays the notification for a threshold rate.

```
device# show notification mac-movement threshold-rate
Threshold-Rate Mac Movement Notification is ENABLED
Configured Threshold-Rate : 5 moves
Configured Sampling-Interval : 30 seconds
Number of entries in the notification table : 100
MAC-Address       from-Port    to-Port    Last Move-Time   Vlan-id
--------------    ---------    -------    --------------   -------
0000.0000.0022    7/1          7/2        Apr 29 18:29:35  10
0000.0000.0021    7/1          7/2        Apr 29 18:29:35  10
0000.0000.0020    7/1          7/2        Apr 29 18:29:35  10
0000.0000.001f    7/1          7/2        Apr 29 18:29:35  10
0000.0000.0024    7/1          7/2        Apr 29 18:29:35  10
0000.0000.001e    7/1          7/2        Apr 29 18:29:35  10
0000.0000.0023    7/1          7/2        Apr 29 18:29:35  10
0000.0000.001d    7/1          7/2        Apr 29 18:29:35  10
0000.0000.001c    7/1          7/2        Apr 29 18:29:35 10
(output truncated)
```

show ntp associations

Displays all the NTP servers and peers association information.

Syntax

show ntp associations [**detail** [*ipv4-address* | *ipv6-address*]]

Parameters

ipv4-address

Displays the NTP servers and peers association information for a specific IPv4 address.

ipv6-address

Displays the NTP servers and peers association information for a specific IPv6 address.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

NTP configuration mode

Interface configuration mode

Command Output

The **show ntp associations** command displays the following information:

Output Field	Description
*	The peer has been declared the system peer and lends its variables to the system variables.
#	This peer is a survivor in the selection algorithm.
+	This peer is a candidate in the combine algorithm.
-	This peer is discarded as outlier in the clustering algorithm.
x	This peer is discarded as 'falseticker' in the selection algorithm.
~	The server or peer is statically configured.
address	IPv4 or IPv6 address of the peer.
ref clock	IPv4 address or first 32 bits of the MD5 hash of the IPv6 address of the peer to which clock is synchronized.
St	Stratum setting for the peer.
when	Time, in seconds, since last NTP packet was received from peer.
poll	Polling interval (seconds).
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to peer, in milliseconds.

Output Field	Description
offset	Relative time difference between a peer clock and a local clock, in milliseconds.
disp	Dispersion.

The **show ntp associations detail** command displays the following information:

Output field	Description
server	Indicates server is statically configured.
symmetric active peer	Indicates peer is statically configured.
symmetric passive peer	Indicates peer is dynamically configured.
sys_peer	This peer is the system peer.
candidate	This peer is chosen as candidate in the combine algorithm.
reject	This peer is rejected by the selection algorithm.
falsetick	This peer is dropped as falseticker by the selection algorithm.
outlier	This peer is dropped as outlyer by the clustering algorithm.
Stratum	Stratum number.
ref ID	IPv4 address or hash of IPv6 address of the upstream time server to which the peer is synchronized.
Time	Last time stamp that the peer received from its master.
our mode	This system's mode relative to peer (active/passive/client/server/bdcast/bdcast client).
peer mode	Mode of peer relative to this system.
our poll intvl	This system's poll interval to this peer.
peer poll intvl	Poll interval of peer to this system.
root delay	The delay along path to root (the final stratum 1 time source).
root disp	Dispersion of path to root.
reach peer	The peer reachability (bit string in octal).
Delay	Round-trip delay to peer.
offset	Offset of a peer clock relative to this clock.
Dispersion	Dispersion of a peer clock.
precision	Precision of a peer clock.
version	Peer NTP version number.
org time	Originate time stamp of the last packet.
rcv time	Receive time stamp of the last packet.
xmt time	Transmit time stamp of the last packet.
filter delay	Round-trip delay in milliseconds of last 8 samples.
filter offset	Clock offset in milliseconds of last 8 samples.
filter error	Approximate error of last 8 samples.

Examples

The following is a sample output of the **show ntp associations** command.

```
device# show ntp associations

        address            ref                clock    st    when    poll    reach    delay
offset     disp
*    ~    172.19.69.1     172.24.114.33     3         25    64         3         2.89     0.234
39377
    ~    2001:235::234
INIT 16 - 64 0 0.00 0.000 15937
* synced, # selected, + candidate, - outlayer, x falseticker, ~ configured
```

The following is a sample output of the **show ntp associations detail** command.

```
device#    show ntp association detail 1.99.40.1

1.99.40.1 configured server, candidate, stratum 3
ref ID 216.45.57.38, time d288de7d.690ca5c7 (10:33:33.1762436551 Pacific Tue Dec 06 2011)
our mode client, peer mode server, our poll intvl 10, peer poll intvl 10,
root delay 0.02618408 msec, root disp 0.10108947, reach 3, root dist 0.23610585
delay 0.92163588 msec, offset 60.77749188 msec, dispersion 70.33842156,
precision 2**-16, version 4
org time        d288defa.b260a71f (10:35:38.2992678687 Pacific Tue Dec 06 2011)
rcv time         d288defa.a2efbd41 (10:35:38.2733620545 Pacific Tue Dec 06 2011)
xmt time         d288defa.a2ae54f8 (10:35:38.2729334008 Pacific Tue Dec 06 2011)
filter delay     0.000 6.7770 6.7773 6.7711 6.7720 6.7736 6.7700 0.9921
filter offset     0.000 19.0047 19.1145 19.2245 19.3313 17.4410 15.4463 60.7777
filter disp     16000.000 16.0005 15.9975 15.9945 15.9915 15.8885 15.8855 0.0030
filter epoch     55683 55683 55685 55687 55689 55691 55693 56748
```

show ntp status

Displays the NTP status.

Syntax

show ntp status

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface management configuration mode

NTP configuration mode

Command Output

The **show ntp status** command displays the following information:

Output field	Description
synchronized	Indicates the system clock is synchronized to NTP server or peer.
stratum	Indicates the stratum number that this system is operating. Range 2..15.
reference	IPv4 address or first 32 bits of the MD5 hash of the IPv6 address of the peer to which clock is synchronized.
precision	Precision of the clock of this system in Hz.
reference time	Reference time stamp.
clock offset	Offset of clock (in milliseconds) to synchronized peer.
root delay	Total delay (in milliseconds) along path to root clock.
root dispersion	Dispersion of root path.
peer dispersion	Dispersion of root path.
system poll interval	Poll interval of the local system.
last update	Time the router last updated its NTP information.
server mode	Status of the NTP server mode for this device.
client mode	Status of the NTP client mode for this device.
master	Status of the master mode.
master stratum	Stratum number that will be used by this device when master is enabled and no upstream time servers are accessible.
panic mode	Status of the panic mode.

Examples

The following is a sample output of the **show ntp status** command.

```
device# show ntp status

Clock is synchronized, stratum 4, reference clock is 10.20.99.174
precision is 2**-16
reference time is D281713A.80000000 (03:21:29.3653007907 GMT+00 Thu Dec 01 2011)
msec, root delay is 24.6646 msec
root dispersion is 130.3376 msec, peer dispersion is 84.3335 msec
system poll interval is 64, last clock update was 26 sec ago
NTP server mode is enabled, NTP client mode is enabled
NTP master mode is disabled, NTP master stratum is 8
NTP is not in panic mode
```

show openflow

Displays the configured OpenFlow parameters.

Syntax

show openflow

Modes

EXEC and Privileged EXEC mode

Global configuration 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 OpenFlow1.3 controller
Controller	Number of controllers

Examples

```
device#show openflow

Administrative Status:       Enabled
Controller Type:             OFV 130
Number of Controllers: 4

Controller 1:
Connection Mode:             passive, TCP
Listening Address:           0.0.0.0
Connection Port:             6633
Connection Status:           TCP_LISTENING
Role:                           Equal
Asynchronous Configuration:  Packet-in (no-match|action|invalid-ttl)
                             Port-status (add|delete|modify)
                             Flow-removed (idle-timeout|hard-timeout|delete|grp-delete)

Controller 2:
Connection Mode:             active, TCP
Controller Address:          10.25.128.243
Connection Port:             2001
Connection Status:           OPENFLOW_ESABLISHED
Role:                           Master
Asynchronous Configuration:  Packet-in (no-match|action|invalid-ttl)
                             Port-status (add|delete|modify)
                             Flow-removed (idle-timeout|hard-timeout|delete|grp-delete)
Controller 3:
Connection Mode:             active, TCP
Controller Address:          10.25.128.242
Connection Port:             6633
Connection Status:           OPENFLOW_ESABLISHED
Role:                           Slave
Asynchronous Configuration:  Port-status (add|delete|modify)

Controller 4:
Connection Mode:             active, TCP
Controller Address:          10.25.128.250
Connection Port:             2002
Connection Status:           OPENFLOW_ESABLISHED
Role:                           Slave
Asynchronous Configuration:  Port-status (add|delete|modify)

Match Capability:
Port, Destination MAC, Vlan, Vlan PCP
Openflow Enabled Ports:      e1/1 e1/2
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow controller

Displays the controller information in a flow.

Syntax

show openflow controller

Modes

EXEC and Privileged EXEC mode

Global configuration 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

```
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
08.0.20	This command was introduced.

show openflow datapath-id

Displays the data path ID assigned to the device.

Syntax

show openflow datapath-id

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Examples

The following example displays openflow flow table entries limit in the flow table.

```
device# configure terminal
device(config)# show openflow datapath-id
datapath-id# 0000001bedb3d0c0
```

History

Release	Command History
08.0.30	This command was introduced.

show openflow flows

Displays the flows information on the OpenFlow ports.

Syntax

show openflow flows

Modes

User EXEC mode

Privileged EXEC mode

Global configuration 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

This command displays the output for flows.

```
device# show openflow flows

Total Number of data packets sent to controller:                    0
Total Number of data bytes sent to controller  :                    0

Total Number of Flows: 1
        Total Number of Port based Flows: 1
        Total Number of L2 Generic Flows: 0
        Total Number of L3 Generic Flows: 0
    ..................
    ..........

Flow ID: 1 Priority: 32768 Status: Active
        Rule:
           In Port:      e2/5
        Instructions: Apply-Actions
                Action: FORWARD
                        Out Port:  e2/1
                Meter id: 1023
        Statistics:
           Total Pkts: 0
           Total Bytes: 0
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow 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*

Parameters

groups *group-id*

Shows details of a specific OpenFlow group.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show openflow groups** command displays the following information:

Output field	Description
Group	Maximum number of group in a flow
Bucket	Number of bucket per group
Action	Number of action per bucket

Examples

```
device#show openflow groups

Max number of groups             : 512
Max number of buckets per group  :  64
Max number of actions per bucket :   1

Max number of SELECT groups          : 120
Max number of buckets in SELECT group: 8
Starting Trunk ID for SELECT groups  : 257
Group id 1

  Transaction id        4043243760
  Type                  ALL
  Packet Count          0
  Byte   Count          0
  Flow   Count          0
  Number of buckets     2
bucket #1
    Weight             0
    Number of actions   1
      action 1: out port: 2/3

  bucket #2
    Weight             0
    Number of actions   1
      action 1: out port: 2/4

----

Total no. of entries printed: 1
```

History

Release version	Command history
08.0.20	This command was introduced.

show openflow interface

Displays the information about the interfaces in a OpenFlow flow.

Syntax

show openflow interface

Modes

User configuration mode

Usage Guidelines

The **show openflow interface** command displays the port, up and down links, tag status, MAC addresses, and the modes.

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
```

History

Release version	Command history
08.0.20	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

Privileged EXEC mode

Global configuration 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 single meter band.

```
device(config)# show openflow meters 1
Meter id: 1

  Transaction id:        1437
  Meter Flags:            KBPS BURST STATS
  Flow Count:            0
  Number of  bands:      1
  In packet count:       -NA-
  In byte count:         0

  Band Type:    DROP

    Rate:                         750000
    Burst size:                   1500          kb
    In packet band count:         -NA-
    In byte band count:           0
```

The following example displays output with two meter bands.

```
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
```

History

Release version	Command history
08.0.20	This command was introduced.

show optic

Displays optic temperature and power information for qualified XFPs, SFPs, and SFP+ installed in a device.

Syntax

show optic [**threshold**] *stackid/slot/port*

Parameters

threshold

Displays the thresholds for a qualified optical transceiver for the specified port.

stackid/slot/port

Displays information about an XFP, SFP, or SFP+ installed in a the particular port.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

NTP configuration mode

Usage Guidelines

NOTE

The **show optic** command takes advantage of information stored and supplied by the manufacturer of the XFP, SFP, or SFP+ transceiver. This information is an optional feature of the Multi-Source Agreement standard defining the optical interface. Not all component suppliers have implemented this feature set. In such cases where the XFP, SFP, or SFP+ transceiver does not supply the information, a "Not Available" message will be displayed for the specific port on which the module is installed.

Command Output

The **show optic** command displays the following information:

Output field	Description
Port	The port number.
Temperature	The operating temperature, in degrees Celsius, of the optical transceiver. The alarm status, as described in the next table.
Tx Power	The transmit power signal, in decibels (dB), of the measured power referenced to one milliwatt (mW). The alarm status, as described in the next table.
Rx Power	The receive power signal, in decibels (dB), of the measured power referenced to one milliwatt (mW). The alarm status, as described in the next table.
Tx Bias Current	The transmit bias power signal, in milliamperes (mA). The alarm status, as described in the next table.

For Temperature, Tx Power, Rx Power, and Tx Bias Current in the show optic command output, values are displayed along with one of the following alarm status values: Low-Alarm, Low-Warn, Normal, High-Warn or High-Alarm. The thresholds that determine these status values are set by the manufacturer of the optical transceivers. The following table describes each of these status values.

TABLE 10 Alarm status value description

Status value	Description
Low-Alarm	Monitored level has dropped below the "low-alarm" threshold set by the manufacturer of the optical transceiver.
Low-Warn	Monitored level has dropped below the "low-warn" threshold set by the manufacturer of the optical transceiver.
Normal	Monitored level is within the "normal" range set by the manufacturer of the optical transceiver.
High-Warn	Monitored level has climbed above the "high-warn" threshold set by the manufacturer of the optical transceiver.
High-Alarm	Monitored level has climbed above the "high-alarm" threshold set by the manufacturer of the optical transceiver.

Examples

The following is a sample output of the **show optic** command.

```
device# show optic 1/1/1

Port         Temperature          Tx Power               Rx Power               Tx Bias Current
+-------+-------------+----------------+----------------+-------------------+
1/1/1           33.2968 C          -005.4075 dBm        -007.4328 dBm       6.306 mA
                Normal                Normal                  Normal                    Normal
```

The following is a sample output of the **show optic threshold** command.

```
device> show optic threshold 2/2/2

Port 2/2/2 sfp monitor thresholds:
Temperature High alarm                  5a00            90.0000 C
Temperature Low alarm                   d300           -45.0000 C
Temperature High warning              5500             85.0000 C
Temperature Low warning               d800            -40.0000 C
Supply Voltage High alarm             9088
Supply Voltage Low alarm              7148
Supply Voltage High warning           8ca0
Supply Voltage Low warning            7530
TX Bias High alarm                          7530             60.000 mA
TX Bias Low alarm                           01f4              1.000 mA
TX Bias High warning                      61a8             50.000 mA
TX Bias Low warning                         05dc              3.000 mA
TX Power High alarm                         1f07            -001.0001 dBm
TX Power Low alarm                          02c4            -011.4996 dBm
TX Power High warning                     18a6            -001.9997 dBm
TX Power Low warning                      037b            -010.5012 dBm
RX Power High alarm                         2710             000.0000 dBm
RX Power Low alarm                          0028            -023.9794 dBm
RX Power High warning                     1f07            -001.0001 dBm
RX Power Low warning                      0032            -023.0102 dBm
```

show packet-inerror-detect

Displays details related to the monitoring for inError packets for configured ports.

Syntax

show packet-inerror-detect

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

Use this show command to view details related to the monitoring of inError packets for configured ports.

Command Output

The **show packet-inerror-detect** command displays the following information:

Output field	Description
Sampling interval	Displays the configured sampling interval.
Port	Identifies a port.
Packet inError count	The number of inError packets received in the sampling interval for the specific port.
State	Displays the status for the specific port.

Examples

The following example displays details related to the monitoring for inError packets for configured ports.

```
device# show packet-inerror-detect

Sampling interval 5 secs

Port    Packet inError count State
1/1/1   30                   Operational
1/1/37  10                   ERR-DISABLED
2/1/1   100                  Operational
```

History

Release version	Command history
07.3.00g	This command was introduced.

show port security

Displays the port security information.

Syntax

show port security [**ethernet** *stack/slot/port* [**restricted-macs**]]

show port security mac [**ethernet** *stack/slot/port* | **unit** *stack-unit-num*]

show port security statistics [**ethernet** *stack/slot/port* | **unit** *stack-unit-num* [**brief**]]

Parameters

ethernet *stack/slot/port*
: Specified Ethernet interface.

restricted-macs
: Displays information about restricted MAC addresses on the specified port.

mac
: Displays secure MAC addresses configured on a device.

unit *stack-unit-num*
: Specifies the stack unit number.

statistics
: Displays port security statistics.

brief
: Displays brief information.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Port security configuration mode

Port security interface configuration mode

Usage Guidelines

The **show port security** command without any options displays the port security settings for all the ports.

Command Output

The **show port security ethernet** command displays the following information:

Output field	Description
Port	The slot and port number of the interface.
Security	Whether port security has been enabled on the interface.
Violation	The action to be undertaken when a security violation occurs, either "shutdown" or "restrict".
Shutdown-Time	The number of seconds a port is shut down following a security violation, if the port is set to "shutdown" when a violation occurs.
Age-Time	The amount of time, in minutes, MAC addresses learned on the port will remain secure.
Max-MAC	The maximum number of secure MAC addresses that can be learned on the interface.

The **show port security mac** command displays the following information:

Output field	Description
Port	The slot and port number of the interface.
Num-Addr	The number of MAC addresses secured on this interface.
Secure-Src-Addr	The secure MAC address.
Resource	Whether the address was secured using a local or global resource.
Age-Left	The number of minutes the MAC address will remain secure.
Shutdown/Time-Left	Whether the interface has been shut down due to a security violation and the number of seconds before it is enabled again.

NOTE
For FCX and ICX switches, after every switchover or failover, the MAC "Age-Left" timer is reset to start because it is not synchronized between the master and the standby stack unit. This behavior is different on the FSX devices where the "Age-Left" timer is not reset.

The **show port security statistics** command displays the following information:

Output field	Description
Port	The slot and port number of the interface.
Total-Addrs	The total number of secure MAC addresses on the interface.
Maximum-Addrs	The maximum number of secure MAC addresses on the interface.
Violation	The number of security violations on the port.
Shutdown/Time-Left	Whether the port has been shut down due to a security violation and the number of seconds before it is enabled again.

Examples

The following example displays the port security settings for port 1/1/1.

```
device# show port security ethernet 1/1/1
Port  Security Violation Shutdown-Time Age-Time  Max-MAC
----- -------- --------- ------------- --------- -------
1/1/1 disabled shutdown   10             10        1
```

The following example shows the list of secure MAC addresses configured on the device.

```
device# show port security mac
Port   Num-Addr  Secure-Src-Addr  Resource  Age-Left  Shutdown/Time-Left
-----  --------  ---------------  --------  --------- ------------------
1/1/1   1        0000.018.747c     Local     10          no
```

The following example displays port security statistics for interface 1/1/1.

```
device# show port security statistics ethernet 1/1/1
Port   Total-Addrs Maximum-Addrs Violation Shutdown/Time-Left
-----  ----------- ------------- --------- ------------------
1/1/1   1          1               0          no
```

show power-savings-statistics

Displays the power savings statistics for the device.

Syntax

show power-savings-statistics

Modes

Global configuration mode

Usage Guidelines

Examples

The following example displays the power savings statistics for the device.

```
device(config)# show power-savings-statistics

Warning - The below is a theoretical calibrated estimation, there may be +- 5% deviation  on the data.


The Power statistics of the switch for the last 5 minutes is


The total power consumption of the switch for the  past 5 minutes  is ------------------------> 76064
milli Watts

The total power savings after enabling EEE for the past 5 minutes  is ------------------------> 3598
milli Watts

The power efficiency of the Switch after Enabling EEE for the past 5 min is ------------------> 4%

                        The Port specific statistics for the past 5 minutes is


Port   EEE-State      Traffic           Power_Rating    Power_Consumed  Power_Conserved
Power_Efficiency
                  Port Utilization%        in mW             in mW          in mW               in%

1/1/1   Enable           0                333               7              257                  77
1/1/2   Enable           0                 33               76             257                  77
1/1/3   Enable           0                333               76             257                  77
1/1/4   Enable           0                333               76             257                  77
1/1/5   Enable           0                333               76             257                  77
1/1/6   Enable           0                333               76             257                  77
1/1/13  Enable           0                333               76             257                  77
1/1/14  Enable           0                333               76             257                  77
1/1/15  Enable           0                333               76             257                  77
1/1/16  Enable           0                333               76             257                  77
1/1/21  Enable           0                333               76             257                  77
1/1/22  Enable           0                333               76             257                  77
1/1/23  Enable           0                333               76             257                  77
1/1/24  Enable           0                333               76             257                  77
1/2/1   Enable           0                  0               0                0                   0
1/2/2   Enable           0                  0               0                0                   0
1/2/3   Enable           0                  0               0                0                   0
1/2/4   Enable           0                  0               0                0                   0
```

History

Release version	Command history
08.0.30	This command was introduced.

show priority-flow-control

Displays the priority flow control (PFC) on the system.

Syntax

show priority-flow-control

Modes

Privileged EXEC mode

Examples

The following example shows the PFC status of all priority groups.

```
Device# show priority-flow-control

Global PFC Status: Enabled
PFC Enabled on PG0
PFC Disabled on PG1
PFC Disabled on PG2
PFC Disabled on PG3
```

The following example shows the PFC status disabled.

```
Device# show priority-flow-control

Global PFC Status: Disabled
```

History

Release version	Command history
8.0.10	This command was introduced.

show protected-link-group

Displays information about the protected link group.

Syntax

show protected-link-group [*group-ID*]

Parameters

group-ID

Displays information about the protected link group identified by the ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show protected-link-group** command displays the following information:

Output field	Description
Group ID	The ID number of the protected link group.
Member Port(s)	The ports that are members of the protected link group.
Configured Active Port	The statically configured active port. If you do not statically configure an active port, this value will be "None".
Current Active Port	The current active port for the protected link group. If all member ports are down, this value will be "None".
Standby Port(s)	The member ports that are on standby.

Examples

The following example shows the output of the **show protected-link-group** command.

```
device# show protected-link-group
Group ID: 1
Member Port(s): ethe 1/1/1 to 1/1/7
Configured Active Port: 1/1/7
Current Active Port: 1/1/7
Standby Port(s): ethe 1/1/5
Total Number of Protected Link Groups: 1
```

show pvlan

Displays the PVLAN information.

Syntax

show pvlan [*vlan-id*]

Parameters

vlan-id

Displays the information for the PVLAN with the specified VLAN ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

VLAN configuration mode

Usage Guidelines

If the VLAN ID is not specified, the command displays the default VLAN ID information. The **show pvlan** command is not supported on software-forwarding platforms.

This command displays the PVLAN configuration with respect to the primary VLAN and its associated secondary VLANs and to display the member ports, promiscous ports, and inter-switch link ports of a PVLAN.

Examples

The following example displays sample output of the **show pvlan** command.

```
device# show pvlan
PVLAN: primary VLAN 100
 Port 1/1/4 1/1/10 1/1/11
Community VLAN 102
 Port 1/1/1 1/1/2 1/1/10 1/1/11
 Promiscuous Port: 1/1/4
 Inter switch link Port: 1/1/10 1/1/11
 BpduGuard enabled Port: 1/1/1 1/1/2
Isolate VLAN 101
 Port 1/1/3 1/1/10 1/1/11
 Promiscuous Port: 1/1/4
 Inter switch link Port: 1/1/10 1/1/11
 BpduGuard enabled Port: 1/1/1 1/1/2
```

show pvstplus-protect-ports

Displays the status of the PVST+ Protect feature, configured by means of the **pvstplus-protect** command.

Syntax

show pvstplus-protect-ports [**ethernet** *unit/slot/port*]

Parameters

ethernet

Specifies an Ethernet port.

unit/slot/port

Number of an Ethernet port. Ranging is allowed by means of the "to" keyword.

Modes

Privileged EXEC mode

Examples

To display the status of PVST+ Protect on all Ethernet interfaces, including the number of dropped PVST+ BPDUs:

```
device# show pvstplus-protect-ports
        Port    PVST Drop Count
        1/1/1   11
        1/1/2   0
        1/1/3   0
        1/1/4   0
```

To display the status of PVST+ Protect on a single Ethernet interface:

```
device# show pvstplus-protect-ports ethernet 1/1/1
PVST-protect is enabled on port 1/1/1.  PVST drop count is 11
```

To display the status of PVST+ Protect on a range of Ethernet interfaces:

```
device# show pvstplus-protect-ports ethernet 1/1/1 to 1/1/4
```

History

Release version	Command history
08.0.30mb	This command was introduced.

show qd-buffer-profile

Displays the user-configurable buffer profile configuration on the device.

Syntax

show qd-buffer-profile { *profile-name* | **all** }

Parameters

profile-name

Displays the user-configurable buffer profile for a specific buffer profile.

all

Displays all the user-configurable buffer profiles on the device.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show qd-buffer-profile** command displays the following information:

Output field	Description
User Buffer Profile	The name of the user-configurable buffer profile.
Port-type	The type of the port: 1 Gbps or 10 Gbps or All.
Total Buffers	The total number of buffers allocated to the port.
Total Descriptors	The total number of descriptors allocated to the port.
Per Queue details	The names of the queues.
Buffers	The total number of buffers allocated to the queue.
Descriptors	The total number of descriptors allocated to the queue.

Examples

The following example displays sample output of the **show qd-buffer-profile** command.

```
device(config)# show qd-buffer-profile OneGigProfile
User Buffer Profile: OneGigProfile Port-type: 1Gig
Total Buffers = 8096 Total Descriptors = 8096
Per Queue details:  Buffers   Descriptors
Traffic Class 0     50        38
Traffic Class 1     50        38
Traffic Class 2     50        38
Traffic Class 3     50        38
Traffic Class 4     50        38
Traffic Class 5     50        38
Traffic Class 6     132       132
Traffic Class 7     20        20
```

show qos egress-buffer-profile

Displays information about egress buffer profiles.

Syntax

show qos egress-buffer-profile [*user-profile-name* | **all**]

Parameters

user-profile-name

Displays information for the specified egress buffer profile.

all

Displays information for all egress buffer profiles configured in the system and a list of all ports attached to any egress buffer profile.

Modes

Global configuration mode

Examples

The following example displays information for an egress buffer profile named egress1.

```
Device(config)# show qos egress-buffer-profile egress1

Egress Buffer Profile: egress1
Ports attached:  1/1/2
Per Queue Details:       Share Level:
Queue 0                  level4-1/9
Queue 1                  level3-1/16
Queue 2                  level3-1/16
Queue 3                  level3-1/16
Queue 4                  level3-1/16
Queue 5                  level3-1/16
Queue 6                  level3-1/16
Queue 7                  level2-1/32
```

History

Release version	Command history
8.0.10	This command was introduced.

show qos ingress-buffer-profile

Displays information about ingress buffer profiles.

Syntax

show qos ingress-buffer-profile [*user-profile-name* | **all**]

Parameters

user-profile-name

Displays information for the specified ingress buffer profile.

all

Displays information for all the ingress buffer profiles configured in the system and a list of their XOFF threshold levels.

Modes

Global configuration mode

Examples

The following example displays information for all the ingress buffer profiles configured in the system and their XOFF threshold levels.

```
Device(config)# show qos ingress-buffer-profile all

Ingress Buffer Profile: i1
Ports attached:  1/1/1
Per PG Detail:           XOFF Level:
PG 0                     level1-1/64
PG 1                     level3-1/16
PG 2                     level4-1/9
PG 3                     level5-1/5

Ingress Buffer Profile: ing1
Ports attached:  --
Per PG Detail:           XOFF Level:
PG 0                     level6-1/3
PG 1                     level2-1/32
PG 2                     level2-1/32
PG 3                     level2-1/32
```

History

Release version	Command history
8.0.20	This command was introduced.

show qos-internal-trunk-queue

Displays the queue-share level of inter-packet-processor (inter-pp) links used to connect master and slave units in ICX 7450 devices.

Syntax

show qos-internal-trunk-queue

Modes

Global configuration mode

Examples

The following example displays the queue-share level applied on egress queues of inter-pp links in a system.

```
device(config)#show qos-internal-trunk-queue
Per Queue Details:       Share Level:
Queue 0                  level7-1/2
Queue 1                  level3-1/16
Queue 2                  level3-1/16
Queue 3                  level3-1/16
Queue 4                  level3-1/16
Queue 5                  level3-1/16
Queue 6                  level3-1/16
Queue 7                  level3-1/16
```

History

Release version	Command history
08.0.20	This command was introduced.

show qos priority-to-pg

Displays priority-to-priority-group (PG) mapping for priority flow control (PFC).

Syntax

show qos priority-to-pg

Modes

Global configuration mode

Usage Guidelines

This command displays priority-to-PG mapping for the following flow control modes:

- PFC
- Symmetrical flow control
- Asymmetrical flow control

Examples

The following example shows priority-to-PG mapping for PFC.

```
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 0
QoS Internal Priority 1 mapped to Priority Group 0
QoS Internal Priority 2 mapped to Priority Group 1
QoS Internal Priority 3 mapped to Priority Group 1
QoS Internal Priority 4 mapped to Priority Group 1
QoS Internal Priority 5 mapped to Priority Group 2
QoS Internal Priority 6 mapped to Priority Group 2
QoS Internal Priority 7 mapped to Priority Group 4
```

The following example shows priority-to-PG mapping for 802.3x (Flow-Control). Honor is enabled.

```
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 0
QoS Internal Priority 1 mapped to Priority Group 0
QoS Internal Priority 2 mapped to Priority Group 1
QoS Internal Priority 3 mapped to Priority Group 1
QoS Internal Priority 4 mapped to Priority Group 1
QoS Internal Priority 5 mapped to Priority Group 2
QoS Internal Priority 6 mapped to Priority Group 2
QoS Internal Priority 7 mapped to Priority Group 4
```

The following example shows priority-to-PG mapping for symmetrical flow control for 802.3x (Flow-Control) in Both mode (Generate and Honor are enabled) or Generate-only mode.

```
Device(config)# symmetrical-flow-control enable
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 7
QoS Internal Priority 1 mapped to Priority Group 7
QoS Internal Priority 2 mapped to Priority Group 7
QoS Internal Priority 3 mapped to Priority Group 7
QoS Internal Priority 4 mapped to Priority Group 7
QoS Internal Priority 5 mapped to Priority Group 2
QoS Internal Priority 6 mapped to Priority Group 2
QoS Internal Priority 7 mapped to Priority Group 4
```

The following example enables flow control on all priorities and shows the priority-to-PG mapping.

```
Device(config)# symmetrical-flow-control enable all
Device(config)# show qos priority-to-pg

QoS Internal Priority 0 mapped to Priority Group 7
QoS Internal Priority 1 mapped to Priority Group 7
QoS Internal Priority 2 mapped to Priority Group 7
QoS Internal Priority 3 mapped to Priority Group 7
QoS Internal Priority 4 mapped to Priority Group 7
QoS Internal Priority 5 mapped to Priority Group 7
QoS Internal Priority 6 mapped to Priority Group 7
QoS Internal Priority 7 mapped to Priority Group 4
```

History

Release version	Command history
8.0.10	This command was introduced.

show qos-profiles

Displays information about QoS profiles

Syntax

show qos-profiles { **all** | *name* }

Parameters

all

Displays information for all profiles.

name

Displays information for the specified profile.

Modes

Global configuration mode

Examples

The following example displays information for all the queues on an FSX device.

```
Device# show qos-profiles all
bandwidth scheduling mechanism: weighted priority
Profile qosp7     : Priority7   bandwidth requested  25% calculated  25%
Profile qosp6     : Priority6   bandwidth requested  15% calculated  15%
Profile qosp5     : Priority5   bandwidth requested  12% calculated  12%
Profile qosp4     : Priority4   bandwidth requested  12% calculated  12%
Profile qosp3     : Priority3   bandwidth requested  10% calculated  10%
Profile qosp2     : Priority2   bandwidth requested  10% calculated  10%
Profile qosp1     : Priority1   bandwidth requested  10% calculated  10%
Profile qosp0     : Priority0   bandwidth requested   6% calculated   6%
```

The following example displays information, including multicast queue weights, for all the queues on an ICX 7450 device.

```
Device#show qos-profiles all
bandwidth scheduling mechanism: mixed weighted priority with strict priority
Unicast Traffic
Profile qosp7     : Priority7(Highest) Set as strict priority
Profile qosp6     : Priority6          Set as strict priority
Profile qosp5     : Priority5          bandwidth requested  25% calculated  25%
Profile qosp4     : Priority4          bandwidth requested  15% calculated  15%
Profile qosp3     : Priority3          bandwidth requested  15% calculated  15%
Profile qosp2     : Priority2          bandwidth requested  15% calculated  15%
Profile qosp1     : Priority1          bandwidth requested  15% calculated  15%
Profile qosp0     : Priority0(Lowest)  bandwidth requested  15% calculated  15%
Multicast Traffic
Profile qosp7+qosp6                    : Priority7(Highest),6      Set as strict priority
Profile qosp5                          : Priority5                 bandwidth requested  25%
calculated  25%
Profile qosp4+qosp3+qosp2              : Priority4,3,2             bandwidth requested  45%
calculated  45%
Profile qosp1+qosp0                    : Priority1,0(Lowest)       bandwidth requested  30%
calculated  30%
```

History

Release version	Command history
08.0.20	This command was modified to display information for multicast queue weights on ICX 7450 and ICX 7750 devices.

show qos-tos

Displays mappings in the DSCP to forwarding priority portion of the QoS information display.

Syntax

show qos-tos

Modes

User EXEC mode

Privilege EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example is a sample ooutput of the **show qos-tos** command.

```
device# show qos-tos
DSCP-Priority map: (dscp = d1d2)
     d2|  0   1   2   3   4   5   6   7   8   9
  d1   |
  -----+-----------------------------------------
   0   |  1
   0   1   1   1
   0   0   0   5
   1
   1   |  6   1   1   1   1   1   4
   2   2  2
   2   |  2   2   2   2   2
   3   3  3   3   3
   3   |  3   3   0
   4   4  4   4   4   4   4
   4   |  7
   5   5  5   5   5   5   5   3
   6
   5   |  6   6   6   6   6   6   6
   7   7  7
   6   |  7   7   7   7
```

show qos scheduler-profile

Displays information about scheduler profiles.

Syntax

show qos scheduler-profile { **all** *user-profile-name*}

Parameters

all

Displays information for all the scheduler profiles configured in the system and a list of all the ports attached to any scheduler profile.

user-profile-name

Displays information for the specified scheduler profile only.

Modes

Global configuration mode

Usage Guidelines

A scheduler profile must be configured before it can be displayed.

Information can be displayed for a maximum of eight scheduler profiles.

On ICX 7750 and ICX 7450 devices this command also displays information for multicast queue weights.

Examples

The following example displays information for a scheduler profile named user1.

```
Device(config)# show qos scheduler-profile user1

User Scheduler Profile: user1   Scheduling Option: Weighted round-robin
Ports attached:  1/1/1
Per Queue details:    Bandwidth%
Traffic Class 0             1%
Traffic Class 1             1%
Traffic Class 2            10%
Traffic Class 3            10%
Traffic Class 4            10%
Traffic Class 5            10%
Traffic Class 6            20%
Traffic Class 7            38%
```

The following example displays information for all the scheduler profiles configured in the system.

```
Device(config)# show qos scheduler-profile all

User Scheduler Profile: user1   Scheduling Option: Weighted round-robin
Ports attached:  1/1/1
Per Queue details:    Bandwidth%
Traffic Class 0             1%
Traffic Class 1             1%
Traffic Class 2            10%
Traffic Class 3            10%
Traffic Class 4            10%
Traffic Class 5            10%
Traffic Class 6            20%
Traffic Class 7            38%

User Scheduler Profile: user2   Scheduling Option: Strict scheduling
Ports attached:  --

User Scheduler Profile: user3   Scheduling Option: Mixed-SP-WRR
Ports attached:  --
Per Queue details:    Bandwidth%
Traffic Class 0            15%
Traffic Class 1            15%
Traffic Class 2            15%
Traffic Class 3            15%
Traffic Class 4            15%
Traffic Class 5            25%
Traffic Class 6            sp
Traffic Class 7            sp

User Scheduler Profile: user4   Scheduling Option: Weighted round-robin
Ports attached:  --
Per Queue details:    Bandwidth%
Traffic Class 0             3%
Traffic Class 1             3%
Traffic Class 2             3%
Traffic Class 3             3%
Traffic Class 4             3%
Traffic Class 5             3%
Traffic Class 6             7%
Traffic Class 7            75%
```

The following example displays information, including multicast queue weights, for a scheduler profile named profle1 on ICX 7450 anf ICX 7750 devices.

```
Device(config)# show qos scheduler-profile profile1
User Scheduler Profile: profile1     Scheduling Option: Weighted round-robin
Unicast per Queue details:      Bandwidth%
Traffic Class 0                      8%
Traffic Class 1                      8%
Traffic Class 2                      8%
Traffic Class 3                      8%
Traffic Class 4                      8%
Traffic Class 5                      8%
Traffic Class 6                      8%
Traffic Class 7                     44%
Multicast per Queue details:    Bandwidth%
Traffic Class 0,1                   16%
Traffic Class 2,3,4                 24%
Traffic Class 5                      8%
Traffic Class 6,7                   52%
```

History

Release version	Command history
8.0.10	This command was introduced.
8.0.20	This command was modified to display information for multicast queue weights on ICX 7450 and ICX 7750 devices.

show rate-limit broadcast

Displays the broadcast limit configured on the device.

Syntax

show rate-limit broadcast

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example is a sample output of the **show rate-limit broadcast** command.

```
device# show rate-limit broadcast

Broadcast/Multicast Limit Settings:
Port    Limit           Packets/Bytes      Packet Type(s)
4       1245184         Bytes              Broadcast + Multicast Bytes
14      65536           Packets            Broadcast only
23      131072          Packets            Broadcast + Multicast
```

show rate-limit input

Displays the fixed rate limiting configuration.

Syntax

show rate-limit input

Modes

User EXEC mode

Privileges EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show rate-limit input** command displays the following information:

Output field	Description
Total rate-limited interface count	The total number of ports that are configured for fixed rate limiting.
Port	The port number.
Configured Input Rate	The maximum rate requested for inbound traffic. The rate is measured in kilobits per second (kbps).
Actual Input Rate	The actual maximum rate provided by the hardware. The rate is measured in bps.

Examples

The following example is a sample output of the **show rate-limit input** command.

```
device#show rate-limit input
Total rate-limited interface count: 5.
    Port       Configured Input Rate    Actual Input Rate
    1/1/1      65000                    65000
    1/1/2      195000                   195000
    1/1/6      1950                     1950
    1/5/2      230432                   230000
    1/5/6      234113                   234000
```

show rate-limit output-shaping

Displays the configured outbound rate shaper on a device.

Syntax

show rate-limit output-shaping

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example is a sample output of the **show rate-limit output-shaping** command.

```
device# show rate-limit output-shaping

Outbound Rate Shaping Limits in Kbps:
        Port     PortMax     Prio0     Prio1     Prio2     Prio3     Prio4     Prio5     Prio6     Prio7
                1                          -                   -
-                     -                    -                   -
-                     -             651
                2                1302                   -                   -
-                     -                    -                   -
-                     -
            15                     651                   -                   -
-                     -                    -                   -
-                     -
```

show rate-limit unknown-unicast

Displays the unknown unicast limit for each port region to which it applies.

Syntax

show rate-limit unknown-unicast

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

This command is supported only on FSX and ICX 7750 devices.

Examples

the following example is a sample output of the **show rate-limit unknown-unicast** command.

```
device# show rate-limit unknown-unicast
Unknown Unicast Limit Settings:
Port Region    Combined Limit    Packets/Bytes
1 - 12         524288            Packets
13 - 24        65536             Bytes
```

show relative-utilization

Displays utilization percentages for an uplink.

Syntax

show relative-utilization *num*

Parameters

num

Specifies the list number. The value can range from 1 to 4.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

After you configure an uplink utilization list, you can display the list to observe the percentage of the uplink bandwidth that each of the downlink ports used during the most recent 30-second port statistics Utilization list for an uplink port interval. The number of packets sent and received between the two ports is listed, as well as the ratio of each individual downlink port packets relative to the total number of packets on the uplink.

Examples

The following is a sample output of the **show relative-utilization** command.

```
device# show relative-utilization 1

uplink: ethe 1/1/1
30-sec total uplink packet count = 2996
packet count ratio (%)
1 /2:100 1/ 3:---
```

show reserved-vlan-map

Displays the assigned VLAN IDs for reserved VLANs.

Syntax

show reserved-vlan-map

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

To view the assigned VLAN IDs for reserved VLANs 4091 and 4092, use the **show reserved-vlan-map** command. The reassigned VLAN IDs also display in the output of the **show running-config** and **show config** commands.

Command Output

The **show reserved-vlan-map** command displays the following information:

Output field	Description
Reserved Purpose	The reason the VLAN is reserved.
Default	The default VLAN ID of the reserved VLAN.
Re-assign	The VLAN ID to which the reserved VLAN was reassigned.
Current	The current VLAN ID for the reserved VLAN.

NOTE
If you reassign a reserved VLAN without saving the configuration and reloading the software, the reassigned VLAN ID will display in the Re-assign column. However, the previously configured or default VLAN ID will display in the Current column until the configuration is saved and the device reloaded.

Examples

The following is a sample output of the **show reserved-vlan-map** command.

```
device> show reserved-vlan-map
Reserved Purpose     Default   Re-assign   Current
 CPU VLAN              4091       10         33
 All Ports VLAN        4092       10         33
```

show rmon

Displays the Remote monitoring (RMON) agent status and information about RMON alarms, events, history, logs, and statistics on the interface.

Syntax

show rmon { **alarm** *alarm-number* | **event** *event-number* | **history** *history-index* | **logs** *event-index* | **statistics** [*number* | *interface-type* | *interface-number*] }

Parameters

alarm

Specifies to display the RMON alarm table.

alarm-number

Specifies the alarm index identification number. Valid values range from 1 through 65535.

event

Specifies to display the RMON event table.

event-number

Specifies the event index identification number. Valid values range from 1 through 65535.

history

Specifies to display the history control data entries for port or interface.

history-number

Specifies the history index identification number of the history entry.

logs

Specifies to display the RMON logging table where RMON log entries are stored.

event-index

Specifies the event index identification number. Valid values range from 1 through 65535.

statistics

Specifies to display the RMON Ethernet statistics; and the statistics group that collects statistics on promiscuous traffic across an interface and total traffic into and out of the agent interface. Valid values range from 1 through 65535.

statistics-number

Specifies the statistics index identification number of the statistics entry.

interface-type

Specifies the ethernet interface or management port.

interface-number

Specifies the interface or management port number.

Modes

Privileged EXEC mode

Global configuration mode

Command Output

The **show rmon** command displays the following information:

Output field	Description
Rising threshold	The sampling value limit, beyond which the rising alarm is triggered.
Falling threshold	The sampling value limit, beyond which the falling alarm is triggered.
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 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. **NOTE** 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). **NOTE** 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 number does not include framing bits but does include FCS octets. **NOTE** 48GC modules do not support count information on jabbers and report 0.
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.

Output field	Description
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 1518 octets pkts	The total number of packets received that were 1024 - 1518 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Event Index	The event index identification number.
Log Index	The log index identification number.
Log Generated time	The time at which the log is generated.
Log Description	Indicates the type of alarm; whether it is a rising or falling alarm.

Examples

The following example shows the output of the **show rmon alarm** command.

```
device(config)# show rmon alarm
Alarm 1 is active, owned by monitor
 Monitors etherStatsPkts.13 every 5 seconds
 Taking absolute samples, last value was 675
 Rising threshold is 100, assigned to event 1
 Falling threshold is 0, assigned to event 1
 On startup enable rising or falling alarm

Alarm 2 is active, owned by monitor
 Monitors etherStatsPkts.2 every 5 seconds
 Taking absolute samples, last value was 414
 Rising threshold is 100, assigned to event 3
 Falling threshold is 0, assigned to event 3
 On startup enable rising or falling alarm
```

The following example shows the output of the **show rmon event** command.

```
device(config)# show rmon event
Event 1 is active, owned by monitor
 Description is testing
 Event firing causes log, community
 Batch ID 0, argument <none>
 Last fired at system up time 3 minutes 52 seconds

Event 2 is active, owned by monitor
 Description is logging
 Event firing causes log and trap, community public
 Batch ID 0, argument <none>
 Last fired at system up time 8 minutes 12 seconds
```

The following example shows the output of the **show rmon history** *history-index* command.

```
device(config)# show rmon history 1
History 1 is active, owned by monitor
 Monitors interface mgmt1 (ifIndex 25) every 30 seconds
 25 buckets were granted to store statistics
```

The following example shows the output of the **show rmon logs** command.

```
device(config)# show rmon logs
 Event Index = 1
     Log Index = 1
     Log Generated time = 00:03:52 (23200)
     Log Description  = rising alarm

 Event Index = 2
     Log Index = 1
     Log Generated time = 00:08:12 (49200)
     Log Description  = rising alarm

 Event Index = 3
     Log Index = 1
     Log Generated time = 00:05:12 (31200)
     Log Description  = rising alarm

 Event Index = 4
     Log Index = 1
     Log Generated time = 00:01:32 (9200)
     Log Description  = falling alarm

     Log Index = 2
     Log Generated time = 00:02:52 (17200)
     Log Description  = rising alarm
```

The following example shows the output of the **show rmon logs** *event-index* command.

```
device(config)# show rmon logs 2
Event Index = 2
     Log Index = 1
     Log Generated time = 00:08:12 (49200)
     Log Description  = rising alarm
```

The following example shows the output of the **show rmon statistics** *number* command.

```
device(config)# show rmon statistics 1
Ethernet statistics 1 is active, owned by monitor
 Interface 1/1/1 (ifIndex 1) counters
           Octets                    0
      Drop events                    0             Packets                    0
   Broadcast pkts                    0      Multicast pkts                    0
 CRC align errors                    0      Undersize pkts                    0
    Oversize pkts                    0           Fragments                    0
          Jabbers                    0          Collisions                    0

 Packet size counters
              64                     0           65 to 127                    0
       128 to 255                    0          256 to 511                    0
      512 to 1023                    0        1024 to 1518                    0
```

The following example shows the statistics of the ethernet interface 1/2/1.

```
device(config)# show rmon statistics ethernet 1/2/1
Ethernet statistics 65 is active, owned by monitor
 Interface 1/2/1 (ifIndex 65) counters
           Octets          30170677670
      Drop events                    0             Packets             72281139
   Broadcast pkts                    0      Multicast pkts             66309417
 CRC align errors                    0      Undersize pkts                    0
    Oversize pkts                    0           Fragments                    0
          Jabbers                    0          Collisions                    0

 Packet size counters
              64                     0           65 to 127             10703415
       128 to 255             19353559          256 to 511             18658554
      512 to 1023             17980963        1024 to 1518              5584648
```

History

Release version	Command history
08.0.20	The **logs** keyword was introduced.

show rmon statistics

Displays textual summary of the statistics for all ports.

Syntax

show rmon statistics [*decimal* | **ethernet** *stackid/slot/port* | **management** *number*]

Parameters

decimal

Specifies the ifIndex.

ethernet *stackid/slot/port*

Displays the RMON statistics for a specific Ethernet interface.

management *number*

Displays the RMON statistics table for the management interface.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

Count information on multicast and broadcast packets, total packets sent, undersized and oversized packets, CRC alignment errors, jabbers, collision, fragments and dropped events is collected for each port on a Brocade Layer 2 Switch or Layer 3 Switch. The statistics group collects statistics on promiscuous traffic across an interface. The interface group collects statistics on total traffic into and out of the agent interface. No configuration is required to activate collection of statistics for the Layer 2 Switch or Layer 3 Switch. This activity is by default automatically activated at system start-up.

Though 48GC modules receive oversized packets and jabbers, they do not support count information for oversized packets and jabbers and the output of the **show rmon statistics** command reports 0 for both of these counters.

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.

Output field	Description
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 alignment 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 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. **NOTE** 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. **NOTE** 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. **NOTE** 48GC modules do not support count information on jabbers and report 0.
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 1518 octets pkts	The total number of packets received that were 1024 - 1518 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.

Examples

The following example is a sample output of the **show rmon statistics** command.

```
device# show rmon statistics

Ethernet statistics 1 is active, owned by monitor
 Interface 1/1/1 (ifIndex 1) counters
          Octets                    0
      Drop events                   0             Packets                   0
   Broadcast pkts                   0      Multicast pkts                   0
 CRC align errors                   0      Undersize pkts                   0
    Oversize pkts                   0           Fragments                   0
         Jabbers                    0          Collisions                   0

 Packet size counters
              64                    0           65 to 127                   0
       128 to 255                   0          256 to 511                   0
      512 to 1023                   0        1024 to 10200                  0

Ethernet statistics 2 is active, owned by monitor
 Interface 1/1/2 (ifIndex 2) counters
          Octets                    0
      Drop events                   0             Packets                   0
   Broadcast pkts                   0      Multicast pkts                   0
 CRC align errors                   0      Undersize pkts                   0
    Oversize pkts                   0           Fragments                   0
         Jabbers                    0          Collisions                   0

 Packet size counters
              64                    0           65 to 127                   0
       128 to 255                   0          256 to 511                   0
      512 to 1023                   0        1024 to 10200                  0
```

The following is a sample output of the **show rmon statistics** command for ifIndex 9.

```
device# show rmon statistics 9
Ethernet statistics 9 is active, owned by monitor
 Interface 1/1/6 (ifIndex 9) counters
          Octets                    0
      Drop events                   0             Packets                   0
   Broadcast pkts                   0      Multicast pkts                   0
 CRC align errors                   0      Undersize pkts                   0
    Oversize pkts                   0           Fragments                   0
         Jabbers                    0          Collisions                   0

 Packet size counters
              64                    0           65 to 127                   0
       128 to 255                   0          256 to 511                   0
      512 to 1023                   0        1024 to 10200                  0
```

show running interface

Displays information about the interface.

Syntax

show running interface [**ethernet** *stack/slot/port* [**to ethernet** *stack/slot/port*] | **loopback** *loopback-number* | **management** *por-id* | **tunnel** *tunnel-id* | **ve** *ve-number*]

Parameters

ethernet *stack/slot/port*

Specifies the configuration on a physical interface. On standalone devices specify the interface ID in the format slot/port-id; on stacked devices you must also specify the stack ID, in the format stack-id/slot/port-id.

to

Specifies information for a range of physical interfaces.

loopback *loopback-number*

Specifies information for a loopback interface.

management *port-id*

Specifiesinformation for a management port.

tunnel *tunnel-id*

Specifies information for a tunnel interface.

ve *ve-number*

Specifies information for a virtual interface.

Modes

Privileged EXEC mode

Examples

The following example displays output from the **show running interface** command, showing that ACLs 10 and f10 are applied to interface 1/1/9 to control neighbor access.

```
Device#show running interface ethernet 1/1/9
interface ethernet 1/1/9
 ip address 15.1.1.5 255.255.255.0
 ip pim-sparse
 ip pim neighbor-filter 10
 ip ospf area 0
 ipv6 address 201::1/64
 ipv6 ospf area 0
 ipv6 pim-sparse
 ipv6 pim neighbor-filter f10
```

History

Release version	Command history
8.0.20a	This command was modified to display neighbor filter information.

show running-config

Displays the current running configuration.

Syntax

show running-config [**interface** { **ethernet** *stack/slot/port* [[**ethernet** *stack/slot/port* **to** *stack/port/slot* | **ethernet** *stack/slot/port*] ...] | **loopback** *loopback-port-num* | **management** *mgmt-port-num* | **tunnel** *tunnel-port-num* | **ve** *ve-port-num* }]

show running-config [**vlan** *vlan-id*]

show running-config [**vrf**]

Parameters

interface
Displays the running configuration for the specified interface type.

ethernet *stack/sport/slot*
Displays the running configuration on the specified Ethernet interface.

to *stack/sport/slot*
Specifies the range of the Ethernet interface for which to display the running configuration.

loopback *loopback-port-num*
Displays the running configuration information for the specified loopback interface.

management *mgmt-port-num*
Displays the running configuration information for the specified management interface.

tunnel *tunnel-port-num*
Displays the running configuration information for the specified tunnel interface.

ve *ve-port-num*
Displays the running configuration information for the specified VE port.

vlan *vlan-id*
Specifies that web management should be enabled on the clients of the specified VLAN.

vrf
Displays the VRF-Lite running configuration.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

Use this command to display the configuration that is currently active on the local switch but which is not saved persistently.

Examples

The following example displays sample output of the **show running-config** command.

```
device(config)# show running-config
Current configuration:
!
ver 08.0.20a
!
stack unit 1
  module 1 icx6610-24-port-management-module
  module 2 icx6610-qsfp-10-port-160g-module
  module 3 icx6610-8-port-10g-dual-mode-module
  stack-trunk 1/2/1 to 1/2/2
  stack-trunk 1/2/6 to 1/2/7
!
!
!
lag red dynamic id 1
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 10 by port
 router-interface ve 10
 multicast port-version 3 ethe 1/1/3
 multicast6 fast-leave-v1
!
vlan 20 by port
 untagged ethe 1/1/5
 multicast port-version 3 ethe 1/1/5
!
vlan 150 by port
!
!
!
!
openflow enable ofv130
!
system-max pim6-hw-mcache 726
!
vrf blue
 rd 10.1.0.1:10
exit-vrf
!
vrf my_vrf
exit-vrf
!
vrf 3
exit-vrf
!
vrf vrf2
exit-vrf
!
vrf mroute
exit-vrf
!
vrf config'
exit-vrf
!
vrf config
exit-vrf
!
(output truncated)
```

show running-config interface ethernet

Displays the status of a specific Ethernet interface.

Syntax

show running-config interface ethernet { *stackid / slot / port* }

Parameters

stackid / slot / port

Stack ID number, slot number, and port number for an existing Ethernet interface.

Modes

Privileged EXEC mode

Examples

This example displays the running configuration for an Ethernet interface including the configured bandwidth.

```
device# show running-config interface ethernet 1/1/9
interface ethernet 1/1/9
 bandwidth 2000
 ip address 10.1.1.5 10.255.255.0
 ip pim
 ip ospf area 0
 ipv6 address 201::1/64
 ipv6 ospf area 0
 ipv6 pim-sparse
 ipv6 pim dr-priority 50
 ipv6 pim border
 ipv6 mld version 2
```

History

Release version	Command history
8.0.30	This command was modified to include configured bandwidth status.

show running-config interface tunnel

Displays the status of a specific tunnel interface.

Syntax

show running-config interface tunnel { *tunnel-number* }

Parameters

tunnel-number

Specifies the tunnel number.

Modes

Privileged EXEC mode

Examples

This example displays the running configuration for a tunnel interface, including the configured bandwidth.

```
device# show running-config interface tunnel 2

interface tunnel 2
 tunnel mode gre ip
 tunnel source 10.0.0.1
 tunnel destination 10.10.0.1
 ip address 10.0.0.1/24
 bandwidth 2000
```

History

Release version	Command history
8.0.30	This command was modified to include configured bandwidth status.

show running-config interface ve

Displays the status of a specific Virtual Ethernet (VE) interface.

Syntax

show running-config interface ve { *vlan_id* }

Parameters

vlan_id

Specifies the configured corresponding VLAN interface.

Modes

Privileged EXEC mode

Examples

This example displays the running configuration for a VE interface, including the configured bandwidth.

```
device# show running-config interface ve 20
interface ve 20
 ip address 10.21.21.22 10.255.255.0
 ip pim-sparse
 ip ospf area 0
 bandwidth 2000
 ipv6 address 2000::2/64
 ipv6 ospf area 0
```

History

Release version	Command history
8.0.30	This command was modified to include configured bandwidth status.

show scheduler-profile

Displays the user-configurable scheduler profile configuration.

Syntax

show scheduler-profile { *user_profile_name* | **all** }

Parameters

user_profile_name

Displays the scheduler profile for the specified profile.

all

Displays all the scheduler profiles configured in the runtime configuration for the system.

Modes

User EXEC mode

Privilege EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following example is a sample output of the **show scheduler-profile all** command.

```
device(config)# show scheduler-profile all

User Profile: profile1  Scheduling Option: Mixed-SP-WRR
Per Queue details:    Bandwidth%
Traffic Class 0       15%
Traffic Class 1       15%
Traffic Class 2       15%
Traffic Class 3       15%
Traffic Class 4       15%
Traffic Class 5       25%
Traffic Class 6       sp
Traffic Class 7       sp
User Profile: profile2  Scheduling Option: Weighted round-robin
Per Queue details:    Bandwidth%
Traffic Class 0       3%
Traffic Class 1       3%
Traffic Class 2       3%
Traffic Class 3       3%
Traffic Class 4       3%
Traffic Class 5       3%
Traffic Class 6       7%
Traffic Class 7       75%
```

show sflow

Displays sFlow configuration and statistics.

Syntax

show sflow

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

You can display the rates you entered for the default sampling rate, module rates, and all sFlow-enabled ports. You can view the agent IP address and several other details.

Command Output

The **show sflow** command displays the following information:

Output field	Description
sFlow version	The version of sFlow enabled on the device, which can be 2 or 5.
sFlow services	The feature state, which can be enabled or disabled.
sFlow agent IP address	The IP address that sFlow is using in the agent_address field of packets sent to the collectors.
Collector	The collector information. The following information is displayed for each collector: • IP address • UDP port If more than one collector is configured, the line above the collectors indicates how many have been configured.
Configured UDP source Port	The UDP source port used to send data to the collector.
Polling interval	The port counter polling interval.
Configured default sampling rate	The configured global sampling rate. If you changed the global sampling rate, the value you entered is shown here. The actual rate calculated by the software based on the value you entered is listed on the next line, "Actual default sampling rate".
Actual default sampling Rate	The actual default sampling rate.
The maximum sFlow sample size	The maximum size of a flow sample sent to the sFlow collector.
exporting cpu-traffic	Indicates whether or not the sFlow agent is configured to export data destined to the CPU (e.g., Telnet sessions) to the sFlow collector: • enabled • disabled
exporting cpu-traffic sample rate	The sampling rate for CPU-directed data, which is the average ratio of the number of incoming packets on an sFlow-enabled port, to the number of flow samples taken from those packets.

Output field	Description
exporting system-info	Indicates whether or not the sFlow agent is configured to export information about CPU and memory usage to the sFlow collector: • enabled • disabled
exporting system-info polling interval	Specifies the interval, in seconds, that sFlow data is sent to the sFlow collector.
UDP packets exported	The number of sFlow export packets the Brocade device has sent. **NOTE** Each UDP packet can contain multiple samples.
sFlow samples collected	The number of sampled packets that have been sent to the collectors.
sFlow ports	The ports on which you enabled sFlow.
Module Sampling Rates	The configured and actual sampling rates for each module. If a module does not have any sFlow-enabled ports, the rates are listed as 0.
Port Sampling Rates	The configured and actual sampling rates for each sFlow-enabled port. The Subsampling factor indicates how many times the sampling rate of the port's module is multiplied to achieve the port's sampling rate. Because of the way the actual sampling rates are computed, the Subsampling factors are always whole numbers.

Examples

The following is a sample output of the **show sflow** command.

```
device# show sflow

sFlow version: 5
sFlow services are enabled.

sFlow agent IP address: 1.1.1.1
3 collector destinations configured:
Collector IP 2.2.2.2, UDP 6343
Collector IP 3.3.3.3, UDP 6343
Collector IP 4.4.4.4, UDP 6343
Configured UDP source port: 9999
Polling interval is 30 seconds.
Configured default sampling rate: 1 per 566 packe
Actual default sampling rate: 1 per 566 packets.
The maximum sFlow sample size: 1200.
Sample mode: All packets including dropped packet
exporting cpu-traffic is enabled.
exporting cpu-traffic sample rate: 18.
exporting system-info is enabled
exporting system-info polling interval: 30 second
22 UDP packets exported
0 sFlow flow samples collected.
sFlow ports: ethe 1/1/1 to 1/1/2
Module Sampling Rates
---------------------
U1:M1 configured rate=300, actual rate=300
Port Sampling Rates
-------------------
Port=1/1/1, configured rate=300, actual rate=300
Port=1/1/2, configured rate=400, actual rate=400
```

show snmp

Displays various SNMP statistics.

Syntax

show snmp [**engineid** | **group** | **server** | **user**]

Parameters

engineid

Displays local and remote SNMP engine IDs.

group

Displays SNMP groups.

server

Displays SNMP server status and trap information

user

Displays SNMPv3 users details.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show snmp engineid** command displays the following information:

Output field	Description
Local SNMP Engine ID	The engine ID that identifies the source or destination of the packet.
Engine Boots	The number of times that the SNMP engine reinitialized itself with the same ID. If the engine ID is modified, the boot count is reset to 0.
Engine time	The current time with the SNMP agent.

The **show snmp group** command displays the following information:

Output field	Description
groupname	The SNMP group name configured using the **snmp-server group** command.
Security model	Indicates which version of SNMP is used for authentication. SNMP version 3 uses a User-Based Security model (RFC 2574) for authentication and privacy services. SNMP version 1 and version 2 use community strings to authenticate SNMP access to management modules. This method can still be used for authentication.

Output field	Description
Security level	• none - If the security model shows v1 or v2, then security level is blank. User names are not used to authenticate users; community strings are used instead. • noauthNoPriv - If the security model shows v3 and user authentication is by user name only. • authNoPriv - If the security model shows v3 and user authentication is by user name and the MD5 or SHA algorithm.

Examples

The following example displays output of the **show snmp engineid** command.

```
device# show snmp engineid
Local SNMP Engine ID: 800007c703748ef88315c0
Engine Boots: 24
Engine time: 1586246
```

The following example displays output of the **show snmp group** command.

```
device# show snmp group
groupname = 1n
security model = v3
security level = authNoPriv
ACL id = 1
readview = r
writeview = exit
notifyview = n

groupname = d3
security model = v3
security level = authNoPriv
ACL id = 3
readview = all
writeview = all
notifyview = all

groupname = d4
security model = v3
security level = authNoPriv
ACL id = 3
readview = <none>
writeview = <none>
notifyview = 3
```

The following example displays output of the **show snmp server** command.

```
device# show snmp server
       Status: Enabled

      Contact: XYZ
     Location: CopyCenter

Max Ifindex per module: 64

Traps
                   Cold start: Enable
                      Link up: Enable
                    Link down: Enable
               Authentication: Enable
         Power supply failure: Enable
                  Fan failure: Enable
              Fan speed change: Enable
               Module inserted: Enable
                Module removed: Enable
Redundant module state change: Enable
          Temperature warning: Enable
                 STP new root: Enable
          STP topology change: Enable
             MAC notification: Enable
        MAC-AUTH notification: Enable
                         VSRP: Enable
                          MRP: Enable
                         UDLD: Enable
                          VRF: Enable
                    link-oam: Enable
                         cfm: Enable
                      nlp-phy: Enable

 Total Trap-Receiver Entries: 0
```

The following example displays output of the **show snmp user** command.

```
device# show snmp user
username = bob
ACL id = 2
group = admin
security model = v3
group ACL id = 0
authtype = md5
authkey = 3aca18d90b8d172760e2dd2e8f59b7fe
privtype = des, privkey = 1088359afb3701730173a6332d406eec
engine ID= 800007c70300e052ab0000
```

show span

Displays the Spanning Tree Protocol information for the device.

Syntax

show span [*number* | **designated-protect** | **fast-uplink-span** | **pvst-mode** | **root-protect**]

show span [**detail** [*number* | **vlan** *vlan-id* [**ethernet** *stackid/slot/port*]]]

show span [**vlan** *vlan-id* [**ethernet** *stackid/slot/port* | **fast-uplink-span**]]

Parameters

number
Displays only the entries after the specified number.

designated-protect
Displays the designated forwarding state disabled.

fast-uplink-span
Displays the status of ports with Fast Uplink Span enabled.

pvst-mode
Displays STP information for the device Per VLAN Spanning Tree (PVST+) compatibility configuration.

root-protect
Displays the STP root guard state.

detail
Displays the detailed STP information for a port.

vlan *vlan-id*
Displays the STP information for a VLAN.

ethernet *stackid/slot/port*
Displays STP information for an Ethernet port.

Modes

The command is supported on all command modes.

Command Output

The **show span** command displays the following information:

Output field	Description
VLAN ID	The port-based VLAN that contains this spanning tree (instance of STP). VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1.
Root ID	The ID assigned by STP to the root bridge for this spanning tree.
Root Cost	The cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0.

Output field	Description
Root Port	The port on this device that connects to the root bridge. If this device is the root bridge, then the value is "Root" instead of a port number.
Priority Hex	This device or VLAN STP priority. The value is shown in hexadecimal format.
Max age sec	The number of seconds this device or VLAN waits for a configuration BPDU from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Hello sec	The interval between each configuration BPDU sent by the root bridge.
Hold sec	The minimum number of seconds that must elapse between transmissions of consecutive Configuration BPDUs on a port.
Fwd dly sec	The number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Last Chang sec	The number of seconds since the last time a topology change occurred.
Chg cnt	The number of times the topology has changed since this device was reloaded.
Bridge Address	The STP address of this device or VLAN.
Port Num	The port number.
Priority Hex	The port STP priority, in hexadecimal format.
Path Cost	The port STP path cost.
State	The port STP state. The state can be one of the following: • BLOCKING - STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs. • DISABLED - The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port. • FORWARDING - STP is allowing the port to send and receive frames. • LISTENING - STP is responding to a topology change and this port is listening for a BPDU from neighboring bridges in order to determine the new topology. No user frames are transmitted or received during this state. • LEARNING - The port has passed through the LISTENING state and will change to the FORWARDING state, depending on the results of STP reconvergence. The port does not transmit or receive user frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table. • DESIGNATED INCONSISTENT - This shows as DESI-INCONS in the output. You can disallow the designated forwarding state on a port in STP 802.1d or 802.1w with the **spanning-tree designated-protect** command. If STP tries to put this port into the designated forwarding role, the device would put this port into a designated inconsistent STP state. This is effectively equivalent to the listening state in STP in which a port cannot transfer any user traffic. When STP no longer marks this port as a designated port, the device automatically removes the port from the designated inconsistent state.
Fwd Trans	The number of times STP has changed the state of this port between BLOCKING and FORWARDING.
Design Cost	The cost to the root bridge as advertised by the designated bridge that is connected to this port. If the designated bridge is the root bridge itself, then the cost is 0. The identity of the designated bridge is shown in the Designated Bridge field.
Designated Root	The root bridge as recognized on this port. The value is the same as the root bridge ID listed in the Root ID field.
Designated Bridge	The designated bridge to which this port is connected. The designated bridge is the device that connects the network segment on the port to the root bridge.

The **show span detail** command displays the following information:

Output field	Description
Active Spanning Tree protocol	The VLAN that contains the listed ports and the active Spanning Tree Protocol.The STP type can be one of the following: • MULTIPLE SPANNNG TREE (MSTP) • GLOBAL SINGLE SPANNING TREE (SSTP)
Bridge identifier	The STP identity of this device.
Active global timers	The global STP timers that are currently active, and their current values. The following timers can be listed: • Hello - The interval between Hello packets. This timer applies only to the root bridge. • Topology Change (TC) - The amount of time during which the topology change flag in Hello packets will be marked, indicating a topology change. This timer applies only to the root bridge. • Topology Change Notification (TCN) - The interval between Topology Change Notification packets sent by a non-root bridge toward the root bridge. This timer applies only to non-root bridges.
Active Timers	The current values for the following timers, if active: • Message age - The number of seconds this port has been waiting for a Hello message from the root bridge. • Forward delay - The number of seconds that have passed since the last topology change and consequent reconvergence. • Hold time - The number of seconds that have elapsed since transmission of the last Configuration BPDU.
BPDUs Sent and Received	The number of BPDUs sent and received on this port since the software was reloaded.

Examples

The following example shows the STP information.

```
device# show span
VLAN 1 BPDU cam_index is 3 and the Master DMA Are(HEX)
STP instance owned by VLAN 1
Global STP (IEEE 802.1D) Parameters:
VLAN      Root              Root    Root    Prio    Max    He-    Ho-    Fwd     Last     Chg    Bridge
ID        ID                Cost    Port    rity    Age    llo    ld     dly     Chang    cnt    Address
                                            Hex     sec    sec    sec    sec     sec
1         800000e0804d4a00  0        Root    8000   20     2      1      15       689      1
00e0804d4a00
Port STP Parameters:
Port          Prio     Path     State        Fwd     Design    Designated        Designated
Num           rity     Cost                  Trans   Cost      Root              Bridge
              Hex
1             80       19       FORWARDING   1       0         800000e0804d4a00  800000e0804d4a00
2             80       0        DISABLED     0       0         0000000000000000  0000000000000000
3             80       0        DISABLED     0       0         0000000000000000  0000000000000000
4             80       0        DISABLED     0       0         0000000000000000  0000000000000000
5             80       19       FORWARDING   1       0         800000e0804d4a00  800000e0804d4a00
6             80       19       BLOCKING     0       0         800000e0804d4a00  800000e0804d4a00
7             80       0        DISABLED     0       0         0000000000000000  0000000000000000
<lines for remaining ports excluded for brevity>
```

The following example shows the detailed STP information.

```
device# show span detail
========================================================================
VLAN 1 - MULTIPLE SPANNING TREE (MSTP) ACTIVE
========================================================================
Bridge identifier - 0x800000e0804d4a00
Active global timers - Hello: 0
Port 1/1/1 is FORWARDING
Port - Path cost: 19, Priority: 128, Root: 0x800000e052a9bb00
Designated - Bridge: 0x800000e052a9bb00, Interface: 1, Path cost: 0
Active Timers - None
BPDUs - Sent: 11, Received: 0
Port 1/1/2 is DISABLED
Port 1/1/3 is DISABLED
Port 1/1/4 is DISABLED <lines for remaining ports excluded for brevity>
```

The following example shows how to display STP information for an individual port in a specific VLAN.

```
device# show span detail vlan 1 ethernet 1/1/1
Port 1/1/1 is FORWARDING
Port - Path cost: 19, Priority: 128, Root: 0x800000e052a9bb00
Designated - Bridge: 0x800000e052a9bb00, Interface: 7, Path cost: 0
Active Timers - None
BPDUs - Sent: 29, Received: 0
```

show span designated-protect

Displays a list of all ports that are not allowed to go into the designated forwarding state.

Syntax

show span designated-protect

Modes

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

Examples

The following example indicates that the designated forwarding state is disallowed for interfaces 2/1/7, 2/1/19, and 2/2/3.

```
device(config)# show span designated-protect
Designated Protection Enabled on:
Ports: (U2/M1)    7 19
Ports: (U2/M2)    3
```

History

Release version	Command history
07.3.00g	This command was introduced.

show stack

Displays information about the units in a stack and a representation of the stack topology.

Syntax

show stack *num*

Parameters

num Displays information for the specified stack unit ID.

Modes

Privileged EXEC mode

Command Output

The **show stack** command displays the following information:

Output field	Description
ID	Specifies the identification number of the stack unit. Each unit in the stack has a unique ID number.
Type	Specifies the type (model) of the stack unit.
Role	Specifies the role of the stack unit. The roles are controller, standby, or member.
Mac Address	Specifies the MAC address of the stack unit. The roles are controller, standby, or member.
Pri	Specifies the priority value assigned to the stack unit. The default value is 128.
State	Specifies whether the stack unit is local or remote. A unit with a State value of Local is the active controller. Units with a State value of Remote are either standby units or member units.
Comment	Indicates if the stack unit is ready (available).

Examples

The following example displays information about a stack with six stack trunks, including a representation of the stack topology.

```
device# show stack

T=21h22m31.3: alone: standalone, D: dynamic cfg, S: static, A=10, B=11, C=12
ID   Type          Role    Mac Address    Pri State   Comment
1  S ICX7750-48XGF active  cc4e.246d.9e00 128 local   Ready
2  S ICX7750-48XGF standby cc4e.246d.8d80   0 remote  Ready
3  S ICX7750-48XGF member  cc4e.246d.9b00   0 remote  Ready
4  S ICX7750-48XGF member  cc4e.246d.9c80   0 remote  Ready
5  S ICX7750-20QXG member  cc4e.2439.2a80   0 remote  Ready
6  S ICX7750-20QXG member  cc4e.2439.3700   0 remote  Ready
7  S ICX7750-20QXG member  cc4e.2439.3880   0 remote  Ready
8  S ICX7750-20QXG member  cc4e.2439.2d00   0 remote  Ready
9  S ICX7750-48XGC member  cc4e.2439.1a00   0 remote  Ready
10 S ICX7750-48XGC member  cc4e.2439.1680   0 remote  Ready
11 S ICX7750-48XGC member  cc4e.2439.1d80   0 remote  Ready
12 S ICX7750-48XGC member  cc4e.2439.1280   0 remote  Ready

    active
     +---+        +---+        +---+        +---+        +---+        +---+
 -2/1| 1 |2/4--3/1| C |3/4==2/1| B |2/4==2/1| A |2/4--2/1| 9 |2/4--2/1| 8 |2/4=
|   +---+        +---+        +---+        +---+        +---+        +---+   |
|                                                                             |
|  standby                                                                    |
|   +---+        +---+        +---+        +---+        +---+        +---+   |
-2/4| 2 |2/1==2/4| 3 |2/1--2/4| 4 |2/1==2/4| 5 |2/1--2/4| 6 |2/1==2/4| 7 |2/1=
     +---+        +---+        +---+        +---+        +---+        +---+
Standby u2 - protocols ready, can failover
Current stack management MAC is cc4e.246d.9e00
```

show stack connection

Displays a representation of stack topology and a detailed connection report that contains information on connection errors or hardware failures.

Syntax

show stack connection

Modes

Privileged EXEC mode

Examples

The following example displays a representation of a ring topology that has seven stack units and details on each of the trunk link connections.

```
device# show stack connection
Probing the topology. Please wait ...
device#
    active
    +---+        +---+        +---+        +---+        +---+        +---+
=2/1| 4 |2/6==2/6| 3 |2/1==2/1| 2 |2/6==2/6| 1 |2/1==2/1| 7 |2/6==2/6| 6 |2/1=
|   +---+        +---+        +---+        +---+        +---+        +---+   |
|                                                                             |
|                                                                      standby  |
|                                                                       +---+   |
-------------------------------------------------------------------------2/1| 5 |2/6=
                                                                        +---+

trunk probe results: 7 links
Link 1: u7 -- u1, num=5
1: 1/2/1 (T0) <---> 7/2/1 (T0)
2: 1/2/2 (T0) <---> 7/2/2 (T0)
3: 1/2/3 (T0) <---> 7/2/3 (T0)
4: 1/2/4 (T0) <---> 7/2/4 (T0)
5: 1/2/5 (T0) <---> 7/2/5 (T0)
Link 2: u2 -- u1, num=5
1: 1/2/6 (T1) <---> 2/2/6 (T1)
2: 1/2/7 (T1) <---> 2/2/7 (T1)
3: 1/2/8 (T1) <---> 2/2/8 (T1)
4: 1/2/9 (T1) <---> 2/2/9 (T1)
5: 1/2/10(T1) <---> 2/2/10(T1)
Link 3: u3 -- u2, num=5
1: 2/2/1 (T0) <---> 3/2/1 (T0)
2: 2/2/2 (T0) <---> 3/2/2 (T0)
3: 2/2/3 (T0) <---> 3/2/3 (T0)
4: 2/2/4 (T0) <---> 3/2/4 (T0)
5: 2/2/5 (T0) <---> 3/2/5 (T0)
Link 4: u4 -- u3, num=5
1: 3/2/6 (T1) <---> 4/2/6 (T1)
2: 3/2/7 (T1) <---> 4/2/7 (T1)
3: 3/2/8 (T1) <---> 4/2/8 (T1)

4: 3/2/9 (T1) <---> 4/2/9 (T1)
5: 3/2/10(T1) <---> 4/2/10(T1)
Link 5: u5 -- u4, num=5
1: 4/2/1 (T0) <---> 5/2/1 (T0)
2: 4/2/2 (T0) <---> 5/2/2 (T0)
3: 4/2/3 (T0) <---> 5/2/3 (T0)
4: 4/2/4 (T0) <---> 5/2/4 (T0)
5: 4/2/5 (T0) <---> 5/2/5 (T0)
Link 6: u6 -- u5, num=5
1: 5/2/6 (T1) <---> 6/2/1 (T0)
2: 5/2/7 (T1) <---> 6/2/2 (T0)
3: 5/2/8 (T1) <---> 6/2/3 (T0)
4: 5/2/9 (T1) <---> 6/2/4 (T0)
5: 5/2/10(T1) <---> 6/2/5 (T0)
Link 7: u7 -- u6, num=5
1: 6/2/6 (T1) <---> 7/2/6 (T1)
2: 6/2/7 (T1) <---> 7/2/7 (T1)
3: 6/2/8 (T1) <---> 7/2/8 (T1)
4: 6/2/9 (T1) <---> 7/2/9 (T1)
5: 6/2/10(T1) <---> 7/2/10(T1)
CPU to CPU packets are fine between 7 units.
```

show stack detail

Displays information on all units in the stack, including the role, MAC address, priority, status, and stack connections for each stack unit.

Syntax

show stack detail

Modes

Privileged EXEC mode

Command Output

The **show stack detail** command displays the following information:

Output field	Description
ID	Specifies the identification number of the stack unit. Each unit in the stack has a unique ID number.
Type	Specifies the type (model) of the stack unit.
Role	Specifies the role of the stack unit. The roles are controller, standby, or member.
Mac Address	Specifies the MAC address of the stack unit. The roles are controller, standby, or member.
Pri	Specifies the priority value assigned to the stack unit. The default value is 128.
State	Specifies whether the stack unit is local or remote. A unit with a State value of Local is the active controller. Units with a State value of Remote are either standby units or member units.
Comment	Indicates if the stack unit is ready (available).
Unit #	Specifies the number assigned to the stack unit. Each unit in the stack has a unique unit number. (This is the same as the ID of the stack unit.)
Stack Port Status	Indicates whether the stack port is connected or disconnected. A port with the up status of up is connected to the stack, and a ports with the status of down (dn) is not connected to the stack.
Neighbors	Indicates units in the stack that are connected together. Each unit in the stack is connected to at least one other stack unit.
System uptime	Indicates the amount of time that the stack unit has been running since the last reset. The System uptime is listed for each unit in the stack.

Examples

The following example displays information on a full ICX 7450 stack containing 12 units, with six different models.

```
device# show stack detail

T=17h38m45.2: alone: standalone, D: dynamic cfg, S: static, A=10, B=11, C=12
ID   Type          Role    Mac Address    Pri State   Comment
1  S ICX7450-24G   active  cc4e.246c.ff80 128 local   Ready
2  S ICX7450-24G   standby cc4e.246d.02c8   0 remote  Ready
3  S ICX7450-24G   member  cc4e.246c.ffd0   0 remote  Ready
4  S ICX7450-24P   member  cc4e.246d.0520   0 remote  Ready
5  S ICX7450-48G   member  cc4e.246d.1c78   0 remote  Ready
6  S ICX7450-48G   member  cc4e.246d.1b78   0 remote  Ready
7  S ICX7450-48G   member  cc4e.246d.1df8   0 remote  Ready
8  S ICX7450-48P   member  cc4e.2489.8640   0 remote  Ready
9  S ICX7450-48GF  member  cc4e.246d.1478   0 remote  Ready
10 D ICX7450-24P   member  cc4e.246d.0638   0 remote  Ready
11 D ICX7450-24P   member  cc4e.246d.0778   0 remote  Ready
12 D ICX7450-48P   member  cc4e.246d.2938   0 remote  Ready

    active       standby
     +---+        +---+        +---+        +---+        +---+        +---+
  3/1| 1 |4/1--3/1| 2 |4/1--3/1| 3 |4/1--3/1| 4 |4/1--3/1| 5 |4/1--3/1| 6 |4/1-
     +---+        +---+        +---+        +---+        +---+        +---+   |
                                                                               |
                                                                               |
     +---+        +---+        +---+        +---+        +---+        +---+   |
     | C |3/1--4/1| B |3/1--4/1| A |3/1--4/1| 9 |3/1--4/1| 8 |3/1--4/1| 7 |3/1-
     +---+        +---+        +---+        +---+        +---+        +---+
Will assign standby in 53 sec due to all ready

Standby u2 - wait for standby assignment due to election
Current stack management MAC is cc4e.246c.ff80

Image-Auto-Copy is Enabled.

      Stack Port Status                  Neighbors
Unit# Stack-port1       Stack-port2      Stack-port1       Stack-port2
1     dn (1/3/1)        up (1/4/1)       none              U2 (2/3/1)
2     up (2/3/1)        up (2/4/1)       U1 (1/4/1)        U3 (3/3/1)
3     up (3/3/1)        up (3/4/1)       U2 (2/4/1)        U4 (4/3/1)
4     up (4/3/1)        up (4/4/1)       U3 (3/4/1)        U5 (5/3/1)
5     up (5/3/1)        up (5/4/1)       U4 (4/4/1)        U6 (6/3/1)
6     up (6/3/1)        up (6/4/1)       U5 (5/4/1)        U7 (7/3/1)
7     up (7/3/1)        up (7/4/1)       U6 (6/4/1)        U8 (8/3/1)
8     up (8/3/1)        up (8/4/1)       U7 (7/4/1)        U9 (9/3/1)
9     up (9/3/1)        up (9/4/1)       U8 (8/4/1)        U10 (10/3/1)
10    up (10/3/1)       up (10/4/1)      U9 (9/4/1)        U11 (11/3/1)
11    up (11/3/1)       up (11/4/1)      U10 (10/4/1)      U12 (12/3/1)
12    up (12/3/1)       none             U11 (11/4/1)      none

Unit# System uptime
1     17 hours 38 minutes 45 seconds
2     17 hours 38 minutes 43 seconds
3     17 hours 38 minutes 45 seconds
4     17 hours 38 minutes 44 seconds
5     17 hours 38 minutes 44 seconds
6     17 hours 38 minutes 44 seconds
7     17 hours 38 minutes 44 seconds
8     17 hours 38 minutes 45 seconds
9     17 hours 38 minutes 43 seconds
10    17 hours 32 minutes 24 seconds
11    1 minutes 9 seconds
12    1 minutes 9 seconds
ICX7450-24 Route
```

show stack failover

Displays information about stack failover.

Syntax

show stack failover

Modes

Privileged EXEC mode

Usage Guidelines

Use the **show stack failover** command to view information about rapid failover for the stack. This command displays if the standby is ready to takeover or not.

Examples

The following example shows which unit is the current standby device and its status.

```
device# show stack failover

Current standby is unit 2. state=ready
Standby u2 - protocols ready, can failover
```

show stack flash

Displays information about flash memory for stack members.

Syntax

show stack flash

Modes

Privileged EXEC mode

Usage Guidelines

Use the **show stack flash** command to display information about flash memory for stack members.

Command Output

The **show stack flash** command displays the following information:

Output field	Description
ID	Specifies the identification number of the stack unit. Each unit in the stack has a unique ID number.
role	Specifies the role of the stack unit. The roles are controller, standby, or member.
priority	Specifies the priority value assigned to the stack unit. The default value is 128.
config	Indicates the port state (up or down) and identifies the port by number (stack-ID/slot/port). A port with the up status of up is connected to the stack, and a ports with the status of down (dn) is not connected to the stack.
The rest of the fields are used for debug purposes only.	

Examples

The following example display flash memory information for an ICX 6610.

```
device# show stack flash
There is no startup-config.old
Stack flash that was read in bootup:
ICX6610-48P, ID =4, role= active, pri=200, config=1, jumbo=X PPVLAN=X S2M=0 FIPS=X
stack p: [0]=4/2/1 [1]=4/2/6 default p: 4/2/1(5) 4/2/6(5), , , hash-chain=X vlan#=X
ve#=X stp#=X
active-chg=0
Current written stack flash:
ICX6610-48P, ID =4, role= active, pri=200, config=1, jumbo=X PPVLAN=X S2M=0 FIPS=X
stack p: [0]=4/2/1 [1]=4/2/6 default p: 4/2/1(5) 4/2/6(5), , , hash-chain=X vlan#=X
ve#=X stp#=X
```

show stack link-sync

Displays the status of the link synchronization.

Syntax

show stack link-sync status

Parameters

status Displays link status information.

Modes

Privileged EXEC mode

Command Output

The **show stack link-sync status** command displays the following information:

Output field	Description
STACKING_LINK_GLOBAL_CTRL messages (sent, received)	Number of global control messages sent and received.
STACKING_LINK_INDIVIDUAL_CTRL messages (sent, received)	Number of individual link control messages sent and received.
STACKING_LINK_STATUS messages (sent, received)	Number of link status control messages sent and received.
STACKING_POE_SCTRL messages (sent, received)	Number of Power over Ethernet (POE) control messages sent and received.
STACKING_POE_STATUS messages (sent, received)	Number of POE status messages sent and received.
global_ctrl_dest	Hexadecimal address of the global control destination.
individual_ctrl_dest	Hexadecimal address of the individual link control destination
status_dest	Number representing the destination status.

Examples

The following example shows link synchronization information for an ICX 6610.

```
device# show stack link-sync status
STACKING_LINK_GLOBAL_CTRL messages sent: 0, received: 0
STACKING_LINK_INDIVIDUAL_CTRL messages sent: 359, received: 0
STACKING_LINK_STATUS messages sent: 22300, received: 128883
STACKING_POE_SCTRL messages sent: 0, received: 0
STACKING_POE_STATUS messages sent: 0, received: 0
global_ctrl_dest: ffffffff
individual_ctrl_dest: ee
status_dest: 30
```

show stack neighbors

Displays information about stack member neighbors.

Syntax

show stack neighbors

Modes

Privileged EXEC mode

Usage Guidelines

Stack neighbors are identified by unit ID for each stack unit.

Command Output

The **show stack neighbors** command displays the following information:

Output field	Description
U#	The identification number of the unit in the stack. Each unit in the stack has a unique identification number.
Stack-port1	Identifies the neighbor stack unit for stack-port1 of the stack unit with this unit identification number (U#). The neighbor stack unit for stack-port1 of each unit in the stack is listed.
Stack-port2	Identifies the neighbor stack unit for stack-port2 of the stack unit with this unit identification number (U#). The neighbor stack unit for stack-port2 of each unit in the stack is listed.

Examples

The following example output is for an ICX 6610 device in a stack with seven members.

```
device# show stack neighbors
U#  Stack-port1             Stack-port2
1   unit7 (7/2/1-7/2/5)     unit2 (2/2/6-2/2/10)
2   unit3 (3/2/1-3/2/5)     unit1 (1/2/6-1/2/10)
3   unit2 (2/2/1-2/2/5)     unit4 (4/2/6-4/2/10)
4   unit5 (5/2/1-5/2/5)     unit3 (3/2/6-3/2/10)
5   unit4 (4/2/1-4/2/5)     unit6 (6/2/1-6/2/5)
6   unit5 (5/2/6-5/2/10)    unit7 (7/2/6-7/2/10)
7   unit1 (1/2/1-1/2/5)     unit6 (6/2/6-6/2/10)
Topology: Ring, 7 unit(s), order: 4 3 2 1 7 6 5
    active
    +-+        +-+        +-+        +-+        +-+        +-+
=2/1|4|2/6==2/6|3|2/1==2/1|2|2/6==2/6|1|2/1==2/1|7|2/6==2/6|6|2/1=
|   +-+        +-+        +-+        +-+        +-+        +-+   |
|                                                                 |
|                                                              standby|
|                                                               +-+   |
-----------------------------------------------------------2/1|5|2/6=
                                                               +-+
```

show stack rel-ipc stats

Displays statistics on reliable Interprocessor Communications (IPC) communications that occur between stack units during a session.

Syntax

show stack rel-ipc stats { **unit** *num* }

Parameters

rel-ipc

Abbreviation for reliable Interprocessor Communications, which designates the proprietary packets exchanged between stack units during a communications session.

stats

Session statistics.

unit *num*

Optional parameter used to specify the stack unit number for which session statistics are to be displayed. If you do not specify a stack unit, session statistics are displayed for all units in the stack.

Modes

Privileged EXEC mode

Usage Guidelines

To display session statistics for a particular stack unit, specify the stack unit using the **unit** *num* parameters.

To display session statistics for all units in the stack, do not specify a stack unit.

Command Output

Depending on whether you specify a stack unit, the **show stack rel-ipc stats** command displays reliable IPC statistics for all units in the stack, or for a single unit in the stack. See the example output below.

Examples

The following example is reliable IPC statistics for an ICX 6610 stack.

```
device# show stack rel-ipc stats
Reliable IPC statistics:
Global statistics:
Pkts rcvd w/no session: 0
Msgs rcvd w/no handler: 0
Unit statistics:
Unit 2 statistics:
Msgs sent: 41384  Msgs received: 14052, Pkt sends failed: 0
Message types sent:
    [9]=21674,        [10]=19703,       [11]=2,           [13]=5,
Message types received:
    [9]=14016,        [10]=2,           [11]=28,          [13]=6,
Session statistics: base-channel, unit 2, channel 0:
Session state: established (last established 15 hours 33 minutes 31 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 14636, Msgs received: 14039
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 30892, Pkts received: 30842
Msg bytes sent: 1828190, Msg bytes received: 1232988
Pkt bytes sent: 2659848, Pkt bytes received: 1763028
Flushes requested: 30, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 888, ACK: 14010, WND: 437, ACK+WND: 0
DAT: 15556, DAT+ACK: 1, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 1069, Zero-window probes sent: 0
Dup ACK pkts rcvd: 1224, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: image-transfer, unit 2, channel 1:
Session state: established (last established 15 hours 11 minutes 2 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 9850, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 9899, Pkts received: 10606
Msg bytes sent: 10124076, Msg bytes received: 8
Pkt bytes sent: 10341308, Pkt bytes received: 127284
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 9897, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 49, Zero-window probes sent: 0
Dup ACK pkts rcvd: 757, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: ACL, unit 2, channel 3:
Session state: established (last established 15 hours 33 minutes 31 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 7011, Msgs received: 4
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 7588, Pkts received: 7617
Msg bytes sent: 629316, Msg bytes received: 5840
Pkt bytes sent: 802504, Pkt bytes received: 107508
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 2
DAT: 7584, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 573, Zero-window probes sent: 0
Dup ACK pkts rcvd: 596, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: sync-reliable, unit 2, channel 4:
Session state: established (last established 15 hours 32 minutes 27 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
```

```
Connection statistics (for current connection, if established):
Msgs sent: 27, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 53, Pkts received: 40
Msg bytes sent: 39420, Msg bytes received: 1460
Pkt bytes sent: 73836, Pkt bytes received: 1944
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 2, ACK: 1, WND: 0, ACK+WND: 0
DAT: 50, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 22, Zero-window probes sent: 0
Dup ACK pkts rcvd: 6, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: rconsole-server-to-2, unit 2, channel 6:
Session state: established (last established 15 hours 33 minutes 30 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 5, Msgs received: 6
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 14, Pkts received: 40
Msg bytes sent: 183, Msg bytes received: 56
Pkt bytes sent: 384, Pkt bytes received: 1052
Flushes requested: 5, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 4, ACK: 5, WND: 0, ACK+WND: 0
DAT: 5, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 0, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Unit 3 statistics:
Msgs sent: 41356  Msgs received: 14007, Pkt sends failed: 0
Message types sent:
    [9]=21623,        [10]=19703,       [11]=29,          [13]=1,
Message types received:
    [9]=14003,        [10]=2,           [13]=2,

Session statistics: base-channel, unit 3, channel 0:
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 14647, Msgs received: 14003
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 31055, Pkts received: 31403
Msg bytes sent: 1801742, Msg bytes received: 1232204
Pkt bytes sent: 2402644, Pkt bytes received: 1877788
Flushes requested: 32, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1269, ACK: 13911, WND: 437, ACK+WND: 0
DAT: 15346, DAT+ACK: 92, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 966, Zero-window probes sent: 0
Dup ACK pkts rcvd: 661, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: image-transfer, unit 3, channel 1:
Session state: established (last established 15 hours 11 minutes 2 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 9850, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 9930, Pkts received: 10599
Msg bytes sent: 10124076, Msg bytes received: 8
Pkt bytes sent: 10457352, Pkt bytes received: 127200
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 9928, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 140, Zero-window probes sent: 0
Dup ACK pkts rcvd: 798, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: ACL, unit 3, channel 3:
```

```
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 7004, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 7447, Pkts received: 7300
Msg bytes sent: 616352, Msg bytes received: 0
Pkt bytes sent: 774304, Pkt bytes received: 87600
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 2, ACK: 0, WND: 0, ACK+WND: 0
DAT: 7445, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 441, Zero-window probes sent: 0
Dup ACK pkts rcvd: 295, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: rconsole-server-to-3, unit 3, channel 7:
Session state: established (last established 15 hours 33 minutes 48 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 1, Msgs received: 2
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 3, Pkts received: 2
Msg bytes sent: 35, Msg bytes received: 20
Pkt bytes sent: 76, Pkt bytes received: 52
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 1, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 0, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Unit 4 statistics:
Msgs sent: 41337  Msgs received: 14035, Pkt sends failed: 0
Message types sent:
    [9]=21632,        [10]=19702,       [11]=2,           [13]=1,
Message types received:
    [9]=14031,        [10]=2,           [13]=2,
Session statistics: base-channel, unit 4, channel 0:
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 14630, Msgs received: 14031
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 30186, Pkts received: 31052
Msg bytes sent: 1801548, Msg bytes received: 1234680
Pkt bytes sent: 2325044, Pkt bytes received: 1857824
Flushes requested: 30, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1199, ACK: 13879, WND: 434, ACK+WND: 4
DAT: 14522, DAT+ACK: 148, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 197, Zero-window probes sent: 0
Dup ACK pkts rcvd: 560, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: image-transfer, unit 4, channel 1:
Session state: established (last established 15 hours 11 minutes 2 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 9850, Msgs received: 1
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 9852, Pkts received: 10675
Msg bytes sent: 10124076, Msg bytes received: 8
Pkt bytes sent: 10284896, Pkt bytes received: 128112
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 1, WND: 0, ACK+WND: 0
DAT: 9850, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 2, Zero-window probes sent: 0
Dup ACK pkts rcvd: 826, Pkts rcvd w/dup data: 0
```

```
Pkts rcvd w/data past window: 0
Session statistics: ACL, unit 4, channel 3:
Session state: established (last established 15 hours 33 minutes 49 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 7004, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 7051, Pkts received: 7240
Msg bytes sent: 616352, Msg bytes received: 0
Pkt bytes sent: 733028, Pkt bytes received: 86880
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 3, ACK: 0, WND: 0, ACK+WND: 0
DAT: 7048, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 44, Zero-window probes sent: 0
Dup ACK pkts rcvd: 234, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics: rconsole-server-to-4, unit 4, channel 8:
Session state: established (last established 15 hours 33 minutes 48 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 1, Msgs received: 2
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 5, Pkts received: 8
Msg bytes sent: 35, Msg bytes received: 20
Pkt bytes sent: 140, Pkt bytes received: 264
Flushes requested: 1, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 2, ACK: 1, WND: 0, ACK+WND: 0
DAT: 2, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 1, Zero-window probes sent: 0
Dup ACK pkts rcvd: 1, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
```

The following example displays session statistics for stack unit 3.

```
device# show stack rel-ipc stats unit 3
Unit 3 statistics:
Msgs sent: 1217  Msgs received: 509, Pkt sends failed: 0
Message types sent:
[9]=1182,         [10]=2,           [11]=2,           [13]=2,
[19]=29,
Message types received:
[9]=506,          [10]=1,           [13]=2,
Session statistics, unit 3, channel 0:
Session state: established (last established 32 minutes 19 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 971, Msgs received: 506
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 1205, Pkts received: 1088
Msg bytes sent: 44281, Msg bytes received: 19308
Pkt bytes sent: 238004, Pkt bytes received: 34652
Flushes requested: 59, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 2, ACK: 504, WND: 7, ACK+WND: 0
DAT: 691, DAT+ACK: 1, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 129, Zero-window probes sent: 0
Dup ACK pkts rcvd: 18, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics, unit 3, channel 2:
Session state: established (last established 32 minutes 17 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 0, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 1, Pkts received: 7
Msg bytes sent: 0, Msg bytes received: 0
Pkt bytes sent: 12, Pkt bytes received: 84
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 0, WND: 0, ACK+WND: 0
DAT: 0, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 7, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics, unit 3, channel 3:
Session state: established (last established 32 minutes 19 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 242, Msgs received: 0
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 243, Pkts received: 246
Msg bytes sent: 8712, Msg bytes received: 0
Pkt bytes sent: 12596, Pkt bytes received: 2952
Flushes requested: 0, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 1, ACK: 0, WND: 0, ACK+WND: 0
DAT: 242, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 4, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
Session statistics, unit 3, channel 6:
Session state: established (last established 32 minutes 17 seconds ago)
Connections established: 1
Remote resets: 0, Reset packets sent: 0
Connection statistics (for current connection, if established):
Msgs sent: 2, Msgs received: 2
Atomic batches sent: 0, Atomic batches received: 0
Pkts sent: 8, Pkts received: 13
Msg bytes sent: 123, Msg bytes received: 20
Pkt bytes sent: 232, Pkt bytes received: 296
```

```
Flushes requested: 2, Suspends: 0, Resumes: 0
Packets sent with data (DAT), ACKs, and window updates (WND):
Other: 5, ACK: 1, WND: 0, ACK+WND: 0
DAT: 2, DAT+ACK: 0, DAT+WND: 0, DAT+ACK+WND: 0
Data retransmits done: 0, Zero-window probes sent: 0
Dup ACK pkts rcvd: 6, Pkts rcvd w/dup data: 0
Pkts rcvd w/data past window: 0
```

show stack resource

Displays resource information for a stack unit.

Syntax

show stack resource

Modes

Privileged EXEC mode

Command Output

The **show stack resource** command displays the following information:

Output field	Description
alloc	Memory allocated
in-use	Memory in use
avail	Available memory
get-fail	The number of get requests that have failed
limit	The maximum memory allocation
get-mem	The number of get-memory requests
size	The size
init	The number of requests initiated

Examples

The following example displays stack resource statistics for an ICX 6610 stack unit.

```
device# show stack resource

                    alloc in-use avail get-fail   limit get-mem size init
register attribute   4800   2710  2090        0  556800    4810  334 2400
general 12B data       32     10    22        0    7424      12   12   32
RB-tree node         4096   2714  1382        0  237568    3026   18 1024
variable length link 3905      4  3901        0  905960       4    8 3905
AU msg dev0          4092      0  4092        0   16368       0   16 4092
AU msg dev1          4092      0  4092        0   16368       0   16 4092
```

show stack stack-ports

Displays status information about stack-ports.

Syntax

show stack stack-ports

Modes

Privileged EXEC mode

Global configuration mode

Command Output

For ICX devices, an equal sign is used to indicate connections between trunk ports and the up port status is listed for all trunked ports. The **show stack stack-ports** command displays the following information:

Output field	Description
U# or ID	Stack unit identification number.
Stack-port 1	Indicates port status (up or down) and identifies the port by number (stack-ID/slot/port).
Stack-port 2	Indicates port status (up or down) and identifies the port by number (stack-ID/slot/port).
Stack-ID up (stack-ID/slot/port)	Indicates status (up or down) for the stack unit and the status (up or down) of all configured stacking ports on the unit by number (stack-ID/slot/port).

Examples

The following output is for an FCX stack with five stacking units.

```
device(config)# show stack stack-ports
ID      Stack-port1       Stack-port2
1       up   (1/2/1)      up   (1/2/2)
2       up   (2/2/1)      up   (2/2/2)
3       up   (3/2/1)      up   (3/3/1)
4       up   (4/2/1)      up   (4/3/1)
5       up   (5/2/1)      up   (5/3/1)
```

The following output is for an ICX 6610 in a seven-unit stack configured in a ring topology.

```
device# show stack stack-ports
    active
    +-+        +-+        +-+        +-+        +-+        +-+
=2/1|4|2/6==2/6|3|2/1==2/1|2|2/6==2/6|1|2/1==2/1|7|2/6==2/6|6|2/1=
|   +-+        +-+        +-+        +-+        +-+        +-+   |
|                                                               |
|                                                          standby|
|                                                           +-+   |
-------------------------------------------------------------2/1|5|2/6=
                                                            +-+

U#  Stack-port1                                  Stack-port2
1   up (1/2/1-1/2/5)                             up (1/2/6-1/2/10)
    up ports: 1/2/1, 1/2/2, 1/2/3, 1/2/4, 1/2/5
    up ports: 1/2/6, 1/2/7, 1/2/8, 1/2/9, 1/2/10
2   up (2/2/1-2/2/5)                             up (2/2/6-2/2/10)
    up ports: 2/2/1, 2/2/2, 2/2/3, 2/2/4, 2/2/5
    up ports: 2/2/6, 2/2/7, 2/2/8, 2/2/9, 2/2/10
3   up (3/2/1-3/2/5)                             up (3/2/6-3/2/10)
    up ports: 3/2/1, 3/2/2, 3/2/3, 3/2/4, 3/2/5
    up ports: 3/2/6, 3/2/7, 3/2/8, 3/2/9, 3/2/10
4   up (4/2/1-4/2/5)                             up (4/2/6-4/2/10)
    up ports: 4/2/1, 4/2/2, 4/2/3, 4/2/4, 4/2/5
    up ports: 4/2/6, 4/2/7, 4/2/8, 4/2/9, 4/2/10
5   up (5/2/1-5/2/5)                             up (5/2/6-5/2/10)
    up ports: 5/2/1, 5/2/2, 5/2/3, 5/2/4, 5/2/5
    up ports: 5/2/6, 5/2/7, 5/2/8, 5/2/9, 5/2/10
6   up (6/2/1-6/2/5)                             up (6/2/6-6/2/10)
    up ports: 6/2/1, 6/2/2, 6/2/3, 6/2/4, 6/2/5
    up ports: 6/2/6, 6/2/7, 6/2/8, 6/2/9, 6/2/10
7   up (7/2/1-7/2/5)                             up (7/2/6-7/2/10)
    up ports: 7/2/1, 7/2/2, 7/2/3, 7/2/4, 7/2/5
    up ports: 7/2/6, 7/2/7, 7/2/8, 7/2/9, 7/2/10
```

show statistics

Displays the packet statistics.

Syntax

show statistics [**brief**] [**management** *num* | **unit** *unit-number*]

show statistics [**brief**] [**ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]]

Parameters

brief
Displays brief output.

management *num*
Displays packet statistics on the management interface.

unit *unit-number*
Displays packet statistics on all ports in a stack unit.

ethernet *stackid/slot/port*
Displays packet statistics on a specific Ethernet interface.

to *stackid/slot/port*
Displays packet statistics on a range of Ethernet interfaces.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

When you use the **brief** option, the output will have only fewer fields.

You can view the packet statistics for a specific Ethernet interface, a list of Ethernet interface, and a range of Ethernet interfaces.

Command Output

The **show statistics ethernet** and **show statistics management**command displays the following information.

NOTE
The output of the **show statistics** command without any options, and the output of the **show statistics** command when using the **brief** option along with **ethernet**, **management**, or **unit** options will display only Port, In Packets, Out Packets, In Errors, and Out Errors fields.

Output field	Description
Port	The port number.
Link	The link state.
State	The STP state.
Dupl	The mode (full-duplex or half-duplex).
Speed	The port speed (10M, 100M, or 1000M).
Trunk	The trunk group number, if the port is a member of a trunk group.
Tag	Whether the port is a tagged member of a VLAN.
Pri	The QoS forwarding priority of the port (level0 - level7).
MAC	The MAC address of the port.
Name	The name of the port, if you assigned a name.
InOctets	The total number of good octets and bad octets received.
OutOctets	The total number of good octets and bad octets sent.
InPkts	The total number of packets received. The count includes rejected and local packets that are not sent to the switching core for transmission. **NOTE** In the output of the **show statistics** command without any options and when using the **brief** option along with the **ethernet**, **management**, or **unit** options, this field is shows as "In Packets".
OutPkts	The total number of good packets sent. The count includes unicast, multicast, and broadcast packets. **NOTE** In the output of the **show statistics** command without any options and when using the **brief** option along with the **ethernet**, **management**, or **unit** options, this field is shows as "Out Packets".
InBroadcastPkts	The total number of good broadcast packets received.
OutBroadcastPkts	The total number of good broadcast packets sent.
InMulticastPkts	The total number of good multicast packets received.
OutMulticastPkts	The total number of good multicast packets sent.
InUnicastPkts	The total number of good unicast packets received.
OutUnicastPkts	The total number of good unicast packets sent.
InBadPkts	The total number of packets received for which one of the following is true: • The CRC was invalid. • The packet was oversized. • Jabbers: The packets were longer than 1518 octets and had a bad FCS. • Fragments: The packets were less than 64 octets long and had a bad FCS. • The packet was undersized (short).
InFragments	The total number of packets received for which both of the following was true: • The length was less than 64 bytes. • The CRC was invalid.
InDiscards	The total number of packets that were received and then dropped due to a lack of receive buffers.

Output field	Description
CRC	The total number of packets received for which all of the following was true: • The data length was between 64 bytes and the maximum allowable frame size. • No Collision or Late Collision was detected. • The CRC was invalid.
Collisions	The total number of packets received in which a Collision event was detected.
InErrors	The total number of packets received that had Alignment errors or phy errors. Excessive errors for some counters usually indicate a problem. When you operate at a halfduplex setting, some data link errors incrementing in Frame Check Sequence (FCS), alignment, runts, and collision counters are normal. Generally, a one percent ratio of errors to total traffic is acceptable for half-duplex connections. If the ratio of errors to input packets is greater than two or three percent, performance degradation could be noticed. In half-duplex environments, it is possible for both the switch and the connected device to sense the wire and transmit at exactly the same time and result in a collision. Collisions may cause runts, FCS, and alignment errors due to the frame not being completely copied to the wire, resulting in fragmented frames. When you operate at full-duplex, errors in FCS, Cyclic Redundancy Checks (CRC), Alignment, and runt counters must be minimal. **NOTE** In the output of the **show statistics** command without any options and when using the **brief** option along with the **ethernet**, **management**, or **unit** options, this field is shows as "In Errors".
OutErrors	The total number of packets sent that had Alignment errors or phy errors. **NOTE** In the output of the **show statistics** command without any options and when using the **brief** option along with the **ethernet**, **management**, or **unit** options, this field is shows as "Out Errors".
LateCollisions	The total number of packets received in which a Collision event was detected, but for which a receive error (Rx Error) event was not detected.
InGiantPkts	The total number of packets for which all of the following was true: • The data length was longer than the maximum allowable frame size. • No Rx Error was detected. **NOTE** Packets are counted for this statistic regardless of whether the CRC is valid or invalid.
InShortPkts	The total number of packets received for which all of the following was true: • The data length was less than 64 bytes. • No Rx Error was detected. • No Collision or Late Collision was detected. **NOTE** Packets are counted for this statistic regardless of whether the CRC is valid or invalid.
InJabber	The total number of packets received for which all of the following was true: • The data length was longer than the maximum allowable frame size. • No Rx Error was detected. • The CRC was invalid.
InFlowCtrlPkts	The total number of flow control packets received.
OutFlowCtrlPkts	The total number of flow control packets transmitted.
InBitsPerSec	The number of bits received per second.
OutBitsPerSec	The number of bits sent per second.
InPktsPerSec	The number of packets received per second.

Output field	Description
OutPktsPerSec	The number of packets sent per second.
InUtilization	The percentage of the port bandwidth used by received traffic.
OutUtilization	The percentage of the port bandwidth used by sent traffic.

Examples

The following is a sample output of the **show statistics brief management** command.

```
device(config)# show statistics brief management 1

Port             In Packets     Out Packets            Trunk     In Errors     Out Errors
mgmt1         39946                          2
2                     0                                    0
Total         39945                          2
2                     0                                        0
```

The following is a sample output of the **show statistics management** command.

```
device# show statistics management 1

Port       Link    State   Dupl Speed Trunk Tag Pvid Pri MAC             Name
mgmt1      Down    None    None None  None  No  None 0   748e.f80c.4100

 Port mgmt1 Counters:
         InOctets                  0          OutOctets                  0
           InPkts                  0            OutPkts                  0
  InBroadcastPkts                  0    OutBroadcastPkts                 0
  InMulticastPkts                  0    OutMulticastPkts                 0
    InUnicastPkts                  0      OutUnicastPkts                 0
        InBadPkts                  0
       InFragments                 0
        InDiscards                 0           OutErrors                 0
               CRC                 0          Collisions                 0
         InErrors                  0      LateCollisions                 0
       InGiantPkts                 0
       InShortPkts                 0
          InJabber                 0
    InFlowCtrlPkts                 0     OutFlowCtrlPkts                 0
      InBitsPerSec                 0       OutBitsPerSec                 0
      InPktsPerSec                 0       OutPktsPerSec                 0
     InUtilization             0.00%      OutUtilization             0.00%
```

The following is a sample output of the **show statistics ethernet** command.

```
device# show statistics ethernet 1/1/1
Port       Link    State      Dupl Speed Trunk  Tag  Pvid Pri MAC             Name
1/1/1      Up      Forward    Half 100M  None   No   1    0   748e.f80c.4100

 Port 1/1/1 Counters:
        InOctets                3200          OutOctets                  256
          InPkts                  50            OutPkts                    4
  InBroadcastPkts                  0    OutBroadcastPkts                   3
  InMulticastPkts                 48    OutMulticastPkts                   0
    InUnicastPkts                  2      OutUnicastPkts                   1
        InBadPkts                  0
      InFragments                  0
       InDiscards                  0           OutErrors                   0
              CRC                  0          Collisions                   0
         InErrors                  0      LateCollisions                   0
      InGiantPkts                  0
      InShortPkts                  0
         InJabber                  0
   InFlowCtrlPkts                  0     OutFlowCtrlPkts                   0
     InBitsPerSec                264       OutBitsPerSec                  16
     InPktsPerSec                  0       OutPktsPerSec                   0
    InUtilization              0.00%      OutUtilization              0.00%
```

show statistics dos-attack

Displays information about ICMP and TCP SYN packets dropped because burst thresholds were exceeded.

Syntax

show statistics dos-attack

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Examples

The following example displays output of the **show statistics dos-attack** command.

```
device# show statistics dos-attack
---------------------------- Local Attack Statistics -------------
ICMP Drop Count     ICMP Block Count     SYN Drop Count     SYN Block Count
---------------     ----------------     --------------     ---------------
0
0
0                                                 0
--------------------------- Transit Attack Statistics ---------------------
Port/VE     ICMP Drop Count     ICMP Block Count     SYN Drop Count     SYN Block Count
-----          ---------------     ----------------     --------------     ---------------
1/3/11                         0                  0               0                0
```

show statistics stack-ports

Displays information about all stacking ports in a stack topology.

Syntax

show statistics stack-ports

Modes

Privileged EXEC mode

Command Output

The **show statistics stack-ports** command displays the following information:

Output field	Description
Port	The number of the port (stack-unit number, slot number, and port number).
In Packets	The number of packets received on this port (incoming packets).
Out Packets	The number of packets sent from this port (outgoing packets).
In Errors	The number of errors received on this port (incoming errors).
Out Errors	The number of errors sent from this port (outgoing errors).

Examples

The following example output is statistics for all stack ports in a stack with seven member units.

```
device# show statistics stack-ports

Port      In Packets   Out Packets   In Errors   Out Errors
1/2/1          22223          4528           0            0
1/2/2          35506          3844           0            0
2/2/1           3161         34173           0            0
2/2/2          24721          3676           0            0
3/2/1           3048         23881           0            0
3/2/2          13540          2857           0            0
4/2/1           2862         13537           0            0
4/2/2           3626          3184           0            0
5/2/1           3183          3621           0            0
5/2/2           3265         13508           0            0
6/2/1          14020          3655           0            0
6/3/1           3652         17705           0            0
7/2/1          17705          3658           0            0
7/3/1           4047         21802           0            0
TOTAL         154559        153629           0            0
```

show statistics traffic-policy

Displays the rate limiting traffic counters and the total packet count and byte count of the traffic filtered by ACL statements.

Syntax

show statistics traffic-policy *TPDname*

Parameters

TPDname

Specifies the name of the traffic policy definition for which you want to display ACL and traffic policy counters.

Modes

User EXEC mode

Privilege EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show statistics traffic-policy** command displays the following information:

Output field	Description
Traffic Policy	The name of the traffic policy.
General Counters	
Port Region #	The port region to which the active traffic policy applies.
Byte Count	The number of bytes (packets in ICX 6650 devices) that were filtered (matched ACL clauses).
Packet Count	The number of packets that were filtered (matched ACL clauses).
Rate Limiting Counters	
Port Region#	The port region to which the active traffic policy applies.
Green Conformance	The number of bytes (packets in ICX 6650 devices) that did not exceed the CIR packet rate.
Yellow Conformance	The number of bytes (packets in ICX 6650 devices) that exceeded the CIR packet rate.
Red Conformance	The number of bytes (packets in ICX 6650 devices) that exceeded the PIR packet rate.

Examples

The following example shows a sample output of the **show statistics traffic-policy** command.

```
device# show statistics traffic-policy abc

Traffic Policy tf125c:

General Counters:
Port Region#         Byte Count       Packet Count
---------------- -------------------- --------------------
0           235400192           1839051
All port regions  235400192           1839051

Rate Limiting Counters (in bytes):
Port Region#    Green/Yellow Conformance    Red Conformance
-------------- --------------------------- --------------------
0               225023872                   10376320
All port regs   225023872                   10376320
```

show stp-bpdu-guard

Displays the BPDU guard state.

Syntax

show stp-bpdu-guard

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

Examples

The following example displays the BPDU guard state.

```
device# show stp-bpdu-guard
BPDU Guard Enabled on:
Interface      Violation
Port 1/1/1     No
Port 1/1/2     No
Port 1/1/3     No
Port 1/1/4     No
Port 1/1/5     No
Port 1/1/6     No
Port 1/1/7     No
Port 1/1/8     No
Port 1/1/9     No
Port 1/1/10    No
Port 1/1/11    No
Port 1/1/12    Yes
Port 1/1/13    No
```

show stp-group

Displays STP topology groups.

Syntax

show stp-group [*group-id*]

Parameters

group-id

Specifies the topology group ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

Examples

The following example displays sample output of the **show stp-group** command.

```
device# show stp-group
Spanning tree Group 1
=================
 master-vlan 2
 member-vlan none

 Common control ports           L2 protocol
  no control ports configured
 Per vlan free ports
 ethernet 1/1/2                  Vlan 2
 ethernet 1/1/3                  Vlan 2
 ethernet 1/1/4                  Vlan 2
```

show stp-protect-ports

Displays the STP protection configuration.

Syntax

show stp-protect-ports [**ethernet** *stackid/slot/port*]

Parameters

ethernet *stackid/slot/port*

Displays the STP protection configuration for a specific Ethernet interface.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

Examples

The following example displays the STP protection configuration.

```
device# show stp-protect-ports
Port          BPDU Drop Count
1/1/3             478
1/1/5             213
1/1/6             0
1/1/12            31
```

The following example shows the STP protection configuration for a particular Ethernet interface.

```
device# show stp-protect-ports ethernet 1/1/3
STP-protect is enabled on port 1/1/3. BPDU drop count is 478
```

show symmetric-flow-control

Displays the status of symmetric flow control as well as the default or configured total buffer limits and XON and XOFF thresholds.

Syntax

show symmetric-flow-control

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following is a sample output of the **show symmetric-flow-control** command.

```
device# show symmetric-flow-control
Symmetric Flow Control Information:
-----------------------------------
SFC: Symmetric Flow Control
Defaults: 1G : Buffers: 272, XOFF Limit: 91, XON Limit: 75
          10G: Buffers: 416, XOFF Limit: 91, XON Limit: 75

     SFC           Total Buffers                    XOFF Limit                        XON Limit
Unit Enabled   1G      10G     1G         10G        1G         10G
---- -------   -------------  --------------------  -------------------
1    No        0       0      0(0%)      0(0%)      0(0%)      0(0%)      0(0%)
```

show telnet

Displays Telnet connection and configuration details.

Syntax

show telnet [**config**]

Parameters

config

Displays Telnet configuration information.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show telnet config** command displays the following information:

Output field	Description
Telnet Server	Telnet server status - enabled or disabled.
Idle timeout	The configured idle timeout of the Telnet server.
Login timeout	The configured login timeout of the Telnet server.
Login retries	The configured number of retries allowed to connect to the Telnet server.
Strict management VRF	Strict management VRF is enabled or disabled for the Telnet server.
Authentication	The authentication is enabled or disabled for the Telnet server.
suppress-reject-message	Whether the connection rejection message is suppressed or not; if a Brocade device denies Telnet management access to the device, the software sends a message to the denied Telnet client.

Examples

The following example displays output of the **show telnet** command showing the Telnet connections and their status.

```
device(config)# show telnet
Console connections (by unit number):
1         established
                you are connecting to this session
                1 minutes 5 seconds in idle
2         established
                1 hours 4 minutes 18 seconds in idle
3         established
                1 hours 4 minutes 15 seconds in idle
4         established
                1 hours 4 minutes 9 seconds in idle
Telnet connections (inbound):
1         closed
2         closed
3         closed
4         closed
5         closed
Telnet connection (outbound):
6         closed
SSH connections:
1         closed
2         closed
3         closed
4         closed
5         closed
```

The following example displays output of the **show telnet config** command showing Telnet configuration details.

```
device(config)# show telnet config
Telnet server                   : Enabled
Idle timeout (minutes)          : 0
Login timeout (minutes)         : 2
Login retries                   : 4
Strict management VRF           : Disabled
Authentication                  : Disabled
suppress-reject-message         : Disabled
Telnet IPv4 clients             : All
Telnet IPv6 clients             : All
Telnet IPv4 access-group        :
Telnet IPv6 access-group        :
```

show topology-group

Displays topology group information.

Syntax

show topology-group [*group-id*]

Parameters

group-id

Displays the information of the topology group of the specified ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

Usage Guidelines

Command Output

The **show topology-group** command displays the following information:

Output field	Description
master-vlan	The master VLAN for the topology group. The settings for STP, MRP, or VSRP on the control ports in the master VLAN apply to all control ports in the member VLANs within the topology group.
member-vlan	The member VLANs in the topology group.
Common control ports	The master VLAN ports that are configured with Layer 2 protocol information. The Layer 2 protocol configuration and state of these ports in the master VLAN applies to the same port numbers in all the member VLANs.
L2 protocol	The Layer 2 protocol configured on the control ports. The Layer 2 protocol can be one of the following: • MRP • STP • VSRP
Per vlan free ports	The ports that are not controlled by the Layer 2 protocol information in the master VLAN.

Examples

The following example displays the topology group information.

```
device# show topology-group
Topology Group 3
================
master-vlan 2
member-vlan none
Common control ports       L2 protocol
ethernet 1/1/1             MRP
ethernet 1/1/2             MRP
ethernet 1/1/5             VSRP
ethernet 1/2/22            VSRP
Per vlan free ports
ethernet 1/2/3             Vlan 2
ethernet 1/1/4             Vlan 2
ethernet 1/2/11            Vlan 2
ethernet 1/2/12            Vlan 2
```

show traffic-policy

Displays traffic policies that are currently defined on the device.

Syntax

show traffic-policy [*TPDname*]

Parameters

TPDname

Specifies the name of the traffic-policy.

Modes

User EXEC mode

Privilege EXEC mode

Global configuration mode

Interface configuration mode

Command Output

The **show traffic-policy** command displays the following information:

Output field	Description
Traffic Policy	The name of the traffic policy.
Metering	Shows whether or not rate limiting was configured as part of the traffic policy: • Enabled - The traffic policy includes a rate limiting configuration. • Disabled - The traffic policy does not include a rate limiting configuration.
Mode	If rate limiting is enabled, this field shows the type of metering enabled on the port: • Fixed Rate-Limiting • Adaptive Rate-Limiting
cir	The committed information rate, in kbps (pkts/s in ICX 6650 devices), for the adaptive rate limiting policy.
cbs	The committed burst size, in bytes (packets in ICX 6650 devices) per second, for the adaptive rate-imiting policy.
pir	The peak information rate, in kbps (pkts/s in ICX 6650 devices), for the adaptive rate limiting policy.
pbs	The peak burst size, in bytes (packets in ICX 6650 devices) per second, for the adaptive rate limiting policy.
Counting	Shows whether or not ACL counting was configured as part of the traffic policy: • Enabled - Traffic policy includes an ACL counting configuration. • Not Enabled - Traffic policy does not include an ACL traffic counting configuration.

Output field	Description
Number of References/Bindings	**NOTE** This field does not apply to FastIron X and ICX 6650 devices. The number of port regions to which this traffic policy applies. For example, if the traffic policy is applied to a trunk group that includes ports e 9/9, 9/10, 9/11, and 9/12, the value in this field would be 2, because these four trunk ports are in two different port regions.

Examples

The following example is a sample output of the **show traffic-policy** command.

```
device# show traffic-policy t_voip

Traffic Policy - t_voip:
Metering Enabled, Parameters:
Mode: Adaptive Rate-Limiting
cir: 100 Pkts/s, cbs: 2000 Pkts, pir: 200 Pkts/s, pbs: 4000 Pkts
Counting Not Enabled
```

show transmit-counter

Displays traffic counter profiles and traffic counter statistics.

Syntax

show transmit-counter { **profiles** | **values** *number* }

Parameters

profiles

Displays the details of the traffic queue profiles.

values *number*

Displays the details of traffic queue counters. Number specifies valid enhanced traffic counter. The value can range from 1 to 64.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Usage Guidelines

This command is supported only on FSX devices.

NOTE

Once the enhanced traffic counters are displayed, the counters are cleared (reset to zero).

Command Output

The **show transmit-counter values** command displays the following information:

Output field	Description
Transmitted frames	
Known Unicast	The number of known unicast packets transmitted.
Multicast & Unknown Unicast	The number of multicast and unknown unicast packets transmitted.
Broadcast	The number of broadcast packets transmitted.
Dropped Frames	

Output field	Description
Bridge Egress Filtered	The number of bridged outbound packets that were filtered and dropped. This number includes the number of packets that were dropped because of any one of the following conditions: • The port was disabled or the link was down. • The port or port region does not belong to the VLAN specified in the transmit counter configuration. • A Layer 2 protocol (e.g., spanning tree) had the port in a Blocked state. • The source port was suppressed for multi-target packets. • The priority queue specified in the traffic counter was not allowed for some other reason. • Unknown unicast and unregistered multicast packets were filtered.
Congestion Drops	The number of outbound packets that were dropped because of traffic congestion.

Examples

The following is a sample output of the **show transmit-counter profiles** command.

```
device# show transmit-counter profiles

Tx Counter     Port(s)           Vlan Id        Priority    Device        Set
1                      1/1-1/12          All            All           Dev 0         Set0
4                      1/18                1                7                Dev 1         Set0
10                     1/13-1/24      100           All           Dev 1         Set10
```

The following is a sample output of the **show transmit-counter values** command.

```
device#show transmit-counter values 1

Transmit Queue Counter Values for Counter 1:
Transmitted Frames:
 Known Unicast               : 17204
 Multicast & Unknown Unicast : 2797
 Broadcast                   : 5
Dropped Frames:
 Bridge Egress Filtered      : 100
 Congestion Drops            : 0
```

show users

Displays the user account information.

Syntax

show users

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Command Output

The **show users** command displays the following information:

Output field	Description
Username	The username of each user.
Password	The password for each user.
Encrypt	Whether the password encryption is enabled or not.
Priv	The privilege level for the user: 0 - Super User level (full read-write access), 4 - Port Configuration level, 5 - Read Only level
Status	Whether the user status is enabled or not.
Expire Time	The password expiration time in days.

Examples

The following example displays output of the **show users** command.

```
device(config)# show users
Username   Password                            Encrypt   Priv Status   Expire Time
=============================================================================
wonka      $1$JVbXZqTW$g9N1/WUipXg6jM6OUKHQZ. enabled   0    enabled  Never
xyz        $1$13zNygo2$vXOKCwghNvXT/YegDawpU0 enabled   0    enabled  Never
aopo       $1$d04FqfAw$W6WiSw6gGJv//C1pvJFpQ. enabled   0    enabled  Never
```

show version

Displays version information of stack members

Syntax

show version

Modes

User EXEC mode

Usage Guidelines

Depending on device support, the serial numbers of the pluggable or fixed modules are displayed in the output. The role of the stack unit and its bootup ID are displayed in the last line of command output. No role is displayed for standalone units.

Examples

The following is an example of the output displayed from the **show version** command, when run on an ICX 7450.

```
device# show version
  Copyright (c) 1996-2016 Brocade Communications Systems, Inc. All rights reserved.
    UNIT 1: compiled on Jun 15 2016 at 02:10:23 labeled as SPR08030b1
      (31817924 bytes) from Primary SPR08030b1.bin
        SW: Version 08.0.30b1T213
      Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215 (spz10106)
  HW: Stackable ICX7450-24-HPOE
  Internal USB: Serial #: 9900614120200136
      Vendor: ATP Electronics, Total size = 1919 MB
==========================================================================
UNIT 1: SL 1: ICX7450-24P POE 24-port Management Module
      Serial  #:CYU3350K004
      License: ICX7450_L3_SOFT_PACKAGE   (LID: eawIIKFmFFJ)
      License Compliance: ICX7450-PREM-LIC-SW is Non-Compliant
      P-ASIC  0: type B548, rev 01  Chip BCM56548_A0
==========================================================================
UNIT 1: SL 2: ICX7400-4X10GF 4-port 40G Module
      Serial  #:CYV3338K099
==========================================================================
UNIT 1: SL 3: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3350K0B5
==========================================================================
UNIT 1: SL 4: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3350K06Y
==========================================================================
 1000 MHz ARM processor ARMv7 88 MHz bus
 8192 KB boot flash memory
 2048 MB code flash memory
 2048 MB DRAM
STACKID 1  system uptime is 2 minute(s) 35 second(s)
The system : started=warm start   reloaded=by "reload"
My stack unit ID = 1, bootup role = alone
*** NOT FOR PRODUCTION ***

ICX7450-24P Router#
```

The following is an example of the output displayed from the **show version** command, when a module is removed form the ICX 7450 device.

```
device# show version
  Copyright (c) 1996-2016 Brocade Communications Systems, Inc. All rights reserved.
    UNIT 1: compiled on Jun 15 2016 at 02:10:23 labeled as SPR08030b1
      (31817924 bytes) from Primary SPR08030b1.bin
        SW: Version 08.0.30b1T213
      Compressed Boot-Monitor Image size = 786944, Version:10.1.06T215 (spz10106)
  HW: Stackable ICX7450-24-HPOE
  Internal USB: Serial #: 9900614120200136
      Vendor: ATP Electronics, Total size = 1919 MB
==========================================================================
UNIT 1: SL 1: ICX7450-24P POE 24-port Management Module
      Serial  #:CYU3350K004
      License: ICX7450_L3_SOFT_PACKAGE   (LID: eawIIKFmFFJ)
      License Compliance: ICX7450-PREM-LIC-SW is Non-Compliant
      P-ASIC  0: type B548, rev 01  Chip BCM56548_A0
==========================================================================
UNIT 1: SL 3: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3350K0B5
==========================================================================
UNIT 1: SL 4: ICX7400-1X40GQ 1-port 40G Module
      Serial  #:CYX3350K06Y
==========================================================================
 1000 MHz ARM processor ARMv7 88 MHz bus
 8192 KB boot flash memory
 2048 MB code flash memory
 2048 MB DRAM
STACKID 1  system uptime is 3 minute(s) 9 second(s)
```

```
The system : started=warm start   reloaded=by "reload"
My stack unit ID = 1, bootup role = alone
*** NOT FOR PRODUCTION ***
ICX7450-24P Router#
```

History

Release version	Command history
08.0.30j	The output of the **show version** command is updated when a module is removed form the device.

show vlan

Displays the VLAN information.

Syntax

show vlan [*vlan-id* [*num*]] [**brief**] [**ethernet** *stackid/slot/port*]

Parameters

vlan-id

Specifies the VLAN ID.

num

Specifies the number of Layer 3 VLAN entries to skip before the display begins.

brief

Displays the VLAN information summary.

ethernet *stackid/slot/port*

Specifies the Ethernet port for which you want to view VLAN details.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

VLAN configuration mode

Command Output

The **show vlan brief** command displays the following information:

Output field	Description
System-max vlan Params	The system maximum VLAN values (maximum, default, and current).
Default vlan Id	The default VLAN ID number.
Total Number of Vlan Configured	The total number of VLANs configured on the device.
VLANs Configured	The VLAN ID numbers of the VLANs configured on the device.

Examples

The following example shows the output of the **show vlan** command..

```
device# show vlan
Total PORT-VLAN entries: 4
Maximum PORT-VLAN entries: 4060
Legend: [Stk=Stack-Unit, S=Slot]
PORT-VLAN 1, Name DEFAULT-VLAN, Priority level0, Spanning tree On
Untagged Ports: (Stk0/S1) 3  4  5  6  7  8  9  10 11 12 13 14
Untagged Ports: (Stk0/S1) 15 16 17 18 19 20 21 22 23 24 25 26
Untagged Ports: (Stk0/S1) 27 28 29 30 31 32 33 34 35 36 37 38
Untagged Ports: (Stk0/S1) 39 40 41 42 43 44 45 46 47 48
Untagged Ports: (Stk0/S2) 1  2
Tagged Ports: None
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: None
Monitoring: Disabled
PORT-VLAN 10, Name [None], Priority level0, Spanning tree On
Untagged Ports: (Stk0/S1) 1
Tagged Ports: None
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: None
Monitoring: Enabled
PORT-VLAN 20, Name [None], Priority level0, Spanning tree On
Untagged Ports: (Stk0/S1) 2
Tagged Ports: None
Uplink Ports: None
DualMode Ports: None
Mac-Vlan Ports: None
Monitoring: Disabled
```

The following example shows the output of the **show vlan brief** command.

```
device# show vlan brief
System-max vlan Params: Max(4095) Default(64) Current(3210)
Default vlan Id :1
Total Number of Vlan Configured :5
VLANs Configured :1 to 4 10
```

The following example shows the output of the port-based **show vlan brief ethernet** command.

```
device# show vlan brief ethernet 1/1/7
Port 1/1/7 is a member of 3 VLANs
VLANs 3 to 4 10
```

show vlan-group

Displays the VLAN group configuration information.

Syntax

show vlan-group [*group-id*]

Parameters

group-id

Displays the VLAN group configuration information for the specified VLAN group ID.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

If you do not specify a group ID, the configuration information for all the configured VLAN groups is displayed.

Examples

The following example displays sample output of the **show vlan-group** command.

```
device# show vlan-group
vlan-group 1 vlan 2 to 20
tagged ethe 1/1/1 to 1/1/2
!
vlan-group 2 vlan 21 to 40
tagged ethe 1/1/1 to 1/1/2
!
```

The following example displays sample output of the **show vlan-group** command for a specific group ID.

```
device# show vlan-group 10
vlan-group 10 vlan 11 to 16
!
```

show voice-vlan

Displays the configuration of a voice VLAN for a particular port or for all ports.

Syntax

show voice-vlan [**ethernet** *stackid/slot/port*]

Parameters

ethernet *stackid/slot/port*

Displays the voice VLAN configuration for the specified Ethernet interface.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Examples

The following is a sample output of the **show voice-vlan** for all ports.

```
device# show voice-vlan

Port ID        Voice-vlan
1/1/2             1001
1/1/8             150
1/1/15            200
```

The following is a sample output of the **show voice-vlan** command for a specific port.

```
device# show voice-vlan ethernet 1/1/2

Voice vlan ID for port 1/1/2: 1001
```

show vrf

Displays IP information for the specified VRF.

Syntax

show vrf [*vrf-name* | **detail** | **resource** [**detail**]]

Parameters

vrf-name

Specifies the VRF for which you want to display the information.

resource

Displays resources used by all VRFs.

detail

Displays detailed VRF instance information. When used along with the **resource** keyword, displays detailed resource information.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VRF configuration mode

Command Output

The **show vrf** command displays the following information:

Output field	Description
VRF *vrf-name*	The name of the VRF.
default RD	The default route distinguisher for the VRF.
Table ID	The table ID for the VRF.
Routes	The total number of IPv4 and IPv6 Unicast routes configured on this VRF.
Configured as management-vrf	Indicates that the specified VRF is configured as a management VRF.
IP Router-Id	The 32-bit number that uniquely identifies the router.
Number of Unicast Routes	The number of Unicast routes configured on this VRF.

Examples

The following is a sample output of the **show vrf** *vrf-name* command.

```
device(config)# show vrf mvrf

VRF mvrf, default RD 1100:1100, Table ID 11
Configured as management-vrf
IP Router-Id: 1.0.0.1
Interfaces:
ve3300 ve3400
Address Family IPv4
Max Routes: 641
Number of Unicast Routes: 2
Address Family IPv6
Max Routes: 64
Number of Unicast Routes: 2
```

show vsrp

Displays the VSRP information.

Syntax

show vsrp [**aware**] [**vlan** *vlan-id* [*vrid-num*] | **vrid** *vrid-num*]

show vsrp [**brief**]

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.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

VSRP VRID configuration mode

Usage Guidelines

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.

Output field	Description
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. • 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.
save-current	The source of VSRP timer values preferred when you save the configuration. This field can have one of the following values: • false: The timer values configured on this device are saved. • true: The timer values most recently received from the master are saved instead of the locally configured values.
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.
Member ports	The ports in the VRID.
Operational ports	The member ports that are currently up.

Output field	Description
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       1/3/2
200        2       1/4/1
```

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    save-current
master    enabled                  disabled            true            false
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 1/2/5 to 1/2/8
Operational ports: ethe 1/2/5 ethe 1/2/8
Forwarding ports: ethe 1/2/5 ethe 1/2/8
Restart ports: 1/2/5(1) 1/2/6(1) 1/2/7(1) 1/2/8(1)
```

show webauth

Displays Web Authentication configuration details.

Syntax

show webauth [**allowed-list** | **authenticating-list** | **blocked-list** | **vlan** *vlan-id* [**passcode** | **webpage**]]

Parameters

allowed-list
Displays a list of hosts that are currently authenticated.

authenticating-list
Displays a list of hosts that are trying to authenticate.

blocked-list
Displays a list of hosts that are currently blocked from any Web Authentication attempt.

vlan *vlan-id*
Displays Web Authentication details on a specific VLAN.

passcode
Displays current dynamic passcode details.

webpage
Displays what text has been configured for Web Authentication pages.

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

Web Authentication configuration mode

Usage Guidelines

The **show webauth** command by itself displays information for all VLANs on which Web Authentication is enabled.

Command Output

The **show webauth** command displays the following information:

Output field	Description
WEB AUTHENTICATION (VLAN #)	Identifies the VLAN on which Web Authentication is enabled.
attempt-max-num	The maximum number of Web Authentication attempts during a cycle.
host-max-num	The maximum number of users that can be authenticated at one time.

Output field	Description
block duration	The number of seconds a user who failed Web Authentication must wait before attempting to be authenticated.
cycle-time	The number of seconds in one Web Authentication cycle.
port-down-authenticated-mac-cleanup	Indicates if this option is enabled or disabled. If enabled, all authenticated users are deauthenticated if all the ports in the VLAN go down.
reauth-time	The number of seconds an authenticated user remains authenticated. Once this timer expires, the user must reauthenticate.
authenticated-mac-age-time	If a user is inactive, this time shows how many seconds a user has before the user-associated MAC address is aged out. The user will be forced to reauthenticate.
dns-filter	Shows the definition of any DNS filter that has been set.
authentication mode	The authentication mode: username and password (default), passcode, captive-portal, or none. Also displays configuration details for the authentication mode.
RADIUS accounting	Whether RADIUS accounting is enabled or disabled.
Trusted port list	The statically-configured trusted ports of the Web Authentication VLAN.
Secure login (HTTPS)	Whether HTTPS is enabled or disabled.
Web Page Customizations	The current configuration for the text that appears on the Web Authentication pages. Either "Custom Text" or "Default Text" displays for each page type: • "Custom Text" means the message for the page has been customized. The custom text is also displayed. • "Default Text" means the default message that ships with the device is used. The actual text on the Web Authentication pages can be displayed using the **show webauth vlan** *vlan-id* **webpage** command.
Host statistics	The authentication status and the number of hosts in each state.

The **show webauth allowed-list** command displays the following information:

Output field	Description
VLAN #: Web Authentication	The ID of the VLAN on which Web Authentication is enabled.
Web Authenticated List MAC Address	The MAC addresses that have been authenticated.
AuthMode	The client is authenticated using internal server or external server.
User Name	The authenticated username.
Configuration Static/Dynamic	If the MAC address was dynamically (passed Web Authentication) or statically (added to the authenticated list using the **add mac** command) authenticated.
Authenticated Duration HH:MM:SS	The remainder of time the MAC address will remain authenticated.
Dynamic ACL	The dynamically assigned ACL.

The **show webauth authenticating-list** command displays the following information:

Output field	Description
VLAN #: Web Authentication	The ID of the VLAN on which Web Authentication is enabled.
MAC Address	The MAC addresses that are trying to be authenticated.
AuthMode	The client is authenticated using internal server or external server.
User Name	The User Name associated with the MAC address.
# of Failed Attempts	Number of authentication attempts that have failed.

Output field	Description
Cycle Time Remaining	The remaining time the user has to be authenticated before the current authentication cycle expires. Once it expires, the user must enter a valid URL again to display the Web Authentication Welcome page.

The **show webauth blocked-list** command displays the following information:

Output field	Description
VLAN #: Web Authentication	The ID of the VLAN on which Web Authentication is enabled.
Web Block List MAC Address	The MAC addresses that have been blocked from Web Authentication.
AuthMode	The client is authenticated using internal server or external server.
User Name	The username associated with the MAC address.
Configuration Static/Dynamic	If the MAC address was dynamically or statically blocked. The **block mac** command statically blocks MAC addresses.
Block Duration Remaining	The remaining time the MAC address has before the user with that MAC address can attempt Web Authentication.

Examples

The following example displays sample output of the **show webauth** command.

```
device#v show webauth
================================================================================
WEB AUTHENTICATION (VLAN 25): Enable
attempt-max-num: 5 (Default)
host-max-num: 0 (Default)
block duration: 90 (Default)
cycle-time: 600 (Default)
port-down-authenticated-mac-cleanup: Enable (Default)
reauth-time: 28800 (Default)
authenticated-mac-age-time: 3600 (Default)
dns-filter: Disable (Default)
authentication mode: username and password (Default)
  authentication methods: radius
   Local user database name: <none>
Radius accounting: Enable (Default)
Trusted port list: None
Secure Login (HTTPS): Enable (Default)
Web Page Customizations:
 Top (Header): Default Text
 Bottom (Footer): Custom Text
  "SNL Copyright 2009"
 Title: Default Text
 Login Button: Custom Text
  "Sign On"
 Web Page Logo: blogo.gif
  align: left (Default)
 Web Page Terms and Conditions: policy1.txt
Host statistics:
 Number of hosts dynamically authenticated: 0
 Number of hosts statically authenticated: 2
 Number of hosts dynamically blocked: 0
 Number of hosts statically blocked: 0
 Number of hosts authenticating: 1
```

The following example displays sample output of the **show webauth allowed-list** command.

```
device# show webauth allowed-list
================================================================================
VLAN 3: Web Authentication, Mode: I = Internal E = External
--------------------------------------------------------------------------------
Web Authenticated List                Configuration   Authenticated Duration  Dynamic
MAC Address       User Name   mode    Static/Dynamic  HH:MM:SS                ACL
--------------------------------------------------------------------------------
000c.2973.a42b    brocade     E       D               1 day, 11:33:16         acl1
1222.0a15.f045    super       E       D               1 day, 11:32:51         acl1
1222.0a15.f044    foundry     E       D               1 day, 11:32:48         acl1
1222.0a15.f043    brocade     E       D               1 day, 11:32:47         acl1
1222.0a15.f042    spirent     E       D               1 day, 11:32:4          acl1
```

The following example displays sample output of the **show webauth authenticating-list** command.

```
device# show webauth authenticating-list
================================================================================
VLAN 3: Web Authentication, AuthMode: I=Internal E=External
--------------------------------------------------------------------------------
Web Authenticating List             # of Failed  Cycle Time Remaining
MAC Address        User Name  mode  Attempts     HH:MM:SS
--------------------------------------------------------------------------------
000c.2973.a42b     N/A        E     0            00:01:36
```

The following example displays sample output of the **show webauth blocked-list** command.

```
device# show webauth blocked-list
================================================================================
VLAN 3: Web Authentication, AuthMode: I=Internal E=External
--------------------------------------------------------------------------------
Block List                       Configuration mode  Block Duration Remaining
MAC Address     User Name  mode  Static/Dynamic
--------------------------------------------------------------------------------
000c.2973.a42b  User1      E     D                   00:00:04
```

The following example displays sample output of the **show webauth vlan** *vlan-id* **passcode** command.

```
device# show webauth vlan 25 passcode
Current Passcode : 1389
This passcode is valid for 35089 seconds
```

The following is a sample output of the **show webauth vlan** *vlan-id* **webpage** command.

```
device# show webauth vlan 25 webpage
================================================
Web Page Customizations (VLAN 25):
  Top (Header): Default Text
    "<h3>Welcome to Brocade Communications, Inc. Web Authentication Homepage</h3>"
  Bottom (Footer): Custom Text
    "Copyright 2009 SNL"
  Title: Default Text
    "Web Authentication"
  Login Button: Custom Text
    "Sign On"
  Web Page Logo: blogo.gif
    align: left (Default)
  Web Page Terms and Conditions: policy1.txt
```

History

Release version	Command history
8.0.40	The output was modified to include "mode" and "Dynamic ACL" fields.

show who

Displays details of the SSH and Telnet connections.

Syntax

show who

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Examples

The following example displays output of the **show who** command.

```
device(config)# show who
Console connections:
        established, privilege super-user, in config mode
        you are connecting to this session
        12 seconds in idle
Telnet server status: Enabled
Telnet connections (inbound):
 1      closed
 2      closed
 3      closed
 4      closed
 5      closed
Telnet connections (outbound):
 6      closed
 7      closed
 8      closed
 9      closed
 10     closed
SSH server status: Disabled
SSH copy-received-cos status: Disabled
SSH connections:
SSH connections (inbound):
 1      closed
 2      closed
 3      closed
 4      closed
 5      closed
SSH connection (outbound):
 6      closed
 7      closed
 8      closed
 9      closed
 10     closed
```

Commands Sn - Z

snmp-client

Restricts SNMP access to a host with the specified IPv4 or IPV6 address.

Syntax

snmp-client {*ip-address* | **ipv6** *ipv6-address* }

no snmp-client {*ip-address* | **ipv6** *ipv6-address* }

Command Default

SNMP access is not restricted.

Parameters

ip-address

The IPv4 address of the host to which the SNMP access is restricted.

ipv6 *ipv6-address*

Specifies the IPv6 address of the host to which the SNMP access is restricted.

Modes

Global configuration mode

Usage Guidelines

You can specify only one IP address with one command. However, you can enter the command ten times to specify up to ten IP addresses.

The **no** form of the command removes the SNMP access restriction.

Examples

The following example shows how to allow SNMP access only to the host with IP address 192.168.10.1.

```
device(config)# snmp-client 192.168.10.1
```

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
```

snmp-server contact

Configures the identification of the contact person for the managed node.

Syntax

snmp-server contact *name*

no snmp-server contact *name*

Command Default

Contact information is not configured.

Parameters

name

The contact name. The name can be up to 255 alphanumeric characters. Spaces are allowed.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the contact information.

Examples

The following example configures the identification of the contact person for the device.

```
device(config)# snmp-server contact Sales
```

snmp-server disable

Disables SNMP MIB support.

Syntax

snmp-server disable mib *table*

no snmp-server disable mib *table*

Command Default

SNMP MIB support is enabled.

Parameters

mib *table*

Disables MIB support for a given table. Support for the following tables can be disabled:

dot1d-tp-fdb

Disables SNMP support for dot1dTpFdbTable.

dot1q-fdb

Disables SNMP support for dot1qFdbTable.

dot1q-tp-fdb

Disables SNMP support for dot1qTpFdbTable.

enet-pw

Disables SNMP support for pwEnetTable.

pw

Disables SNMP support for pwTable.

vll-ep

Disables SNMP support for fdryVllEndPointTable.

vpls-ep-vlan-ext

Disables SNMP support for brcdVplsEndptVlanExtStatsTable.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command enables SNMP MIB support.

Examples

The following example disables dot1d-tp-fdb MIB support.

```
decice(config)# snmp-server disable mib dot1d-tp-fdb
```

snmp-server enable

Configures SNMP access only to specific clients.

Syntax

snmp-server enable ethernet *stack/slot/port* [**to** *stack/slot/port* | [**ethernet** *stack/slot/port* **to** *stack/slot/port* | **ethernet** *stack/slot/port*] ...]

no snmp-server enable ethernet *stack/slot/port* [**to** *stack/slot/port* | [**ethernet** *stack/slot/port* **to** *stack/slot/port* | **ethernet** *stack/slot/port*] ...]

snmp-server enable vlan *vlan-id*

no snmp-server enable vlan *vlan-id*

Command Default

SNMP access is not restricted.

Parameters

ethernet *stack/slot/port*
Specifies the Ethernet interface on which web management should be enabled.

to *stack/slot/port*
Specifies the range of Ethernet interfaces.

vlan *vlan-id*
Specifies that web management should be enabled on the clients of the specified VLAN.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the SNMP access restriction.

Examples

The following example configures the SNMP access only to a client in VLAN 40.

```
device(config)# snmp-server enable vlan 40
```

The following example configures SNMP access to a range of Ethernet interfaces.

```
device(config)# snmp-server enable ethernet 1/1/1 to ethernet 1/1/5
```

snmp-server enable mib

Enables MIB support for SNMP server.

Syntax

snmp-server enable mib *mib-name*

no snmp-server enable mib *mib-name*

Command Default

MIB support is enabled by default.

Parameters

mib-name

Enables support for one of the following MIBs:

np-qos-stat

Enables SNMP support for brcdNPQosStatTable.

tm-dest-qstat

Enables SNMP support for brcdTMDestUcastQStatTable.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables the SNMP MIB support.

Examples

The following example enables the brcdTMDestUcastQStatTable MIB support.

```
device(config)# snmp-server enable mib tm-dest-qstat
```

snmp-server enable traps

Enables SNMP traps for various events.

Syntax

snmp-server enable traps *event*

no snmp-server enable traps *event*

Command Default

Traps are enabled by default.

Parameters

event

The event for which the traps should be enabled. Enables the traps for one of the following events:

authentication
Generates the trap when the authentication occurs.

cold-start
Generates the trap after a cold start.

fan-failure
Generates the trap when there is a fan failure and when the issue is resolved.

fan-speed-change
Generates the trap when there is a change in fan speed.

link-down
Generates the trap when the link is down.

link-oam
Generates the trap for link OAM.

link-up
Generates the trap when the link is up.

mac-authentication
Generates the trap when a MAC address is added or deleted.

mac-notification
Generates the trap after a MAC authentication.

metro-ring
Generates the trap when there is a change in the Metro Ring configuration.

module-inserted
Generates the trap when a module is inserted.

module-removed
Generates the trap when a module is removed.

new-root

nlp-phy-40g
Generates the trap during PHY calibration on the 40-Gbps and 4x10-Gbps stack ports.

power-supply-failure
Generates the trap when there is a power supply failure and when the issue is resolved.

redundant-module

temperature
Generates the trap when there is a temperature change.

topology-change

udld

vsrp

Modes

Global configuration mode

Usage Guidelines

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

Examples

The following example enables SNMP traps on the device for MAC notification globally.

```
device(config)# snmp-server enable traps mac-notification
```

History

Release version	Command history
08.0.10	The **mac-notification** keyword was added.

snmp-server enable traps holddown-time

Configures the wait time before starting to send SNMP traps.

Syntax

snmp-server enable traps holddown-time *time*

no snmp-server enable traps holddown-time *time*

Command Default

The default hold-down time is 60 seconds.

Parameters

time

The time in seconds. The valid range is from 1 through 600 seconds. The default is 60 seconds.

Modes

Global configuration mode

Usage Guidelines

When a Brocade device starts up, the software waits for Layer 2 convergence (STP) and Layer 3 convergence (OSPF) before beginning to send SNMP traps to external SNMP servers. Until convergence occurs, the device may not be able to reach the servers, in which case the messages are lost.

By default, a Brocade device uses a one-minute hold-down time to wait for the convergence to occur before starting to send SNMP traps. After the hold-down time expires, the device sends the traps, including traps such as "cold start" or "warm start" that occur before the hold-down time expires.

When you have a stack of eight or more units, you must increase the trap hold-down time from the default (60 seconds) to five minutes (300 seconds). This will prevent the loss of initial boot traps.

The **no** form of the command changes the hold-down time to the default value.

Examples

The following example changes the hold-down time for SNMP traps to 30 seconds.

```
device(config)# snmp-server enable traps holddown-time 30
```

snmp-server enable traps mac-notification

Enables the MAC-notification trap whenever a MAC address event is generated on a device or an interface.

Syntax

snmp-server enable traps mac-notification

no snmp-server enable traps mac-notification

Command Default

MAC-notification traps are disabled on the device.

Modes

Global configuration

Interface configuration

Usage Guidelines

The **no** form of this command disables SNMP traps for MAC-notification events. The SNMP MAC-notification trap functionality allows an SNMPv3 trap to be sent to the SNMP manager when MAC addresses are added or deleted in the device.

Examples

The following example enables SNMP traps on the device for MAC-notification globally:

```
device(config)# snmp-server enable traps mac-notification
```

The following example disables SNMP traps on the device for MAC-notification globally:

```
device(config)# no snmp-server enable traps mac-notification
```

History

Release version	Command history
08.0.10	This command was introduced.

snmp-server engineid local

Modifies the default SNMPv3 engine ID.

Syntax

snmp-server engineid local *engineid-string*

no snmp-server engineid local *engineid-string*

Command Default

A default engine ID is generated during system startup.

Parameters

engineid-string

Specifies the engine ID as a hexidecimal character string with an even number of characters.

Modes

Global configuration mode

Usage Guidelines

The default engine ID guarantees the uniqueness of the engine ID for SNMP version 3. A default engine ID is generated during system startup. To determine the default engine ID of the device, enter the **show snmp engineid** command. Use the **snmp-server engineid local** command to change the default engine ID.

Each user localized key depends on the SNMP server engine ID, so all users must be reconfigured whenever the SNMP server engine ID changes.

NOTE
Because the current implementation of SNMP version 3 does not support Notification, remote engine IDs cannot be configured at this time.

The **engineid-string** variable consists of 11 octets, entered as hexadecimal values. There are two hexadecimal characters in each octet. There must be an even number of hexadecimal characters in an engine ID.

The default engine ID has a maximum of 11 octets:

- Octets 1 through 4 represent the agent's SNMP management private enterprise number as assigned by the Internet Assigned Numbers Authority (IANA). The most significant bit of Octet 1 is "1". For example, "000007c7" is the ID for Brocade Communications, Inc. in hexadecimal. With Octet 1 always equal to "1", the first four octets in the default engine ID is always "800007c7" (which is 1991 in decimal).
- Octet 5 is always 03 in hexadecimal and indicates that the next set of values represents a MAC address.
- Octets 6 through 11 form the MAC address of the lowest port in the management module.

The engine ID must be a unique number among the various SNMP engines in the management domain.

The **no** form of the command sets the engine ID to the default.

Examples

The following example shows how to change the default engine ID.

```
device(config)# snmp-server engineid local 800007c70300e05290ab60
```

snmp-server group

Creates user-defined groups for SNMPv1/v2c/v3 and configures read, write, and notify permissions to access the MIB view.

Syntax

snmp-server group *groupname* { **v1** | **v2c** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *viewname*]

no snmp-server group *groupname* { **v1** | **v2c** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *viewname*]

snmp-server group *groupname* **v3** { **auth** | **noauth** | **priv** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *viewname*]

no snmp-server group *groupname* **v3** { **auth** | **noauth** | **priv** } [**access** { *standard-ACL-id* | **ipv6** *ipv6-ACL-name* }] [**notify** *viewname*] [**read** *viewname*] [**write** *viewname*]

Command Default

Six default groups are supported to associate the default SNMPv3 user groups and the default SNMPv1/v2c community groups with the view configuration.

NOTE
This command is not used for SNMP version 1 and SNMP version 2. In these versions, groups and group views are created internally using community strings. When a community string is created, two groups are created, based on the community string name. One group is for SNMP version 1 packets, while the other is for SNMP version 2 packets.

Parameters

groupname
Specifies the name of the SNMP group to be created.

v1
Specifies SNMP version 1.

v2c
Specifies SNMP version 2.

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.

access
Specifies an access list associated with the SNMP group.

standard-ACL-id
Specifies the standard IP access list and allows the incoming SNMP packets to be filtered based on the standard ACL attached to the group.

ipv6
Specifies the IPv6 ACL for the SNMP group.

ipv6-ACL-name
Specifies the IPv6 access list and allows incoming SNMP packets to be filtered based on the IPv6 ACL attached to the group.

notify *viewname*
Specifies the name of the view that enables you to provide access to the MIB for trap or inform. This allows the administrators to restrict the scope of varbind objects that will be part of the notification. All of the varbinds need to be in the included view for the notification to be created.

read *viewname*
Specifies the name of the view that enables you to provide read access.

write *viewname*
Specifies the name of the view that enables you to provide both read and write access.

viewname
Specifies the name of the view to which the SNMP group members have access. If no view is specified, then the group has no access to the MIB. The default viewname is "all", which allows access to the entire MIB.

Modes

Global configuration mode

Usage Guidelines

Maximum number of SNMP groups supported is 10.

The **no** form of the command removes the configured SNMP server group.

Examples

The following example creates SNMP server group entries for SNMPv3 user group with auth permission.

```
device(config)# snmp-server group admin v3 auth ipv6 acl_1 read all write all notify all
```

History

Release version	Command history
08.0.20a	The **ipv6** *ipv6-ACL-name* keyword-argument pair 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
```

snmp-server legacy

Configures legacy values for SNMP MIBs.

Syntax

snmp-server legacy { **iftype** | **module-type** }

no snmp-server legacy { **iftype** | **module-type** }

Command Default

SNMP MIBs have the user-configured values.

Parameters

iftype

Configures to the use of legacy Ethernet interface names for ifType.

module-type

Configures to the use of legacy enum values for snAgentConfigModuleType.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command changes the settings back to the non-legacy values.

Examples

The following example configures to the use of legacy Ethernet interface names for ifType.

```
device(config)# snmp-server legacy iftype
```

snmp-server location

Configures the SNMP server location.

Syntax

snmp-server location *string*

no snmp-server location *string*

Command Default

The SNMP server location is not configured.

Parameters

string

The physical location of the server. The string can be up to 255 alphanumeric characters. Spaces are allowed.

Modes

Global configuration mode

Usage Guidelines

You can configure a location for a device and save the information locally in the configuration file for future reference. This information is not required for system operation but is suggested.

The **no** form of the command removes the configured location.

Examples

The following example configures the physical location of the SNMP server.

```
device(config)# snmp-server location United States
```

snmp-server max-ifindex-per-module

Configures the maximum number of ifindexes per module.

Syntax

snmp-server max-ifindex-per-module *number*

no snmp-server max-ifindex-per-module *number*

Command Default

The system assigns 64 indexes to each module on the device.

Parameters

number

Specifies the maximum number of ifindexes per module (20, 40 or 64).

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the maximum number of ifindexes per module as 64.

SNMP Management Information Base (MIB) uses Interface Index (ifIndex) to assign a unique value to each port on a module or slot. You can assign 20, 40, and 64 ifindexes per module.

Examples

The following example configures the number of ifindexes per module to 40.

```
device(config)# snmp-server max-ifindex-per-module 40
```

snmp-server preserve-statistics

Decouples SNMP statistics from CLI-based statistics.

Syntax

snmp-server preserve-statistics

no snmp-server preserve-statistics

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command couples the SNMP statistics from the CLI based statistics.

Examples

The following example shows how to decouple SNMP statistics from CLI-based statistics.

```
device(config)# snmp-server preserve-statistics
```

snmp-server pw-check

Controls password check on file operation MIB objects.

Syntax

snmp-server pw-check

no snmp-server pw-check

Command Default

Password check is not configured.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the password check on file operation MIB objects.

Once the password check is enabled, if a third-party SNMP management application does not add a password to the password field when it sends SNMP set requests to a device, by default the device rejects the request.

Examples

The following example configures password check on file operation MIB objects.

```
device(config)# snmp-server pw-check
```

snmp-server trap-source

Configures an interface as the source for all traps.

Syntax

snmp-server trap-source { **ethernet** *stackid/slot/port* | **loopback** *number* | **ve** *number* }

no snmp-server trap-source { **ethernet** *stackid/slot/port* | **loopback** *number* | **ve** *number* }

Command Default

SNMP trap generator is not configured.

Parameters

ethernet *stackid/slot/port*

Specifies the Ethernet interface address used as a source for all traps.

loopback *number*

Specifies the loopback interface address used as a source for all traps.

ve *number*

Specifies the Virtual Ethernet interface address used as a source for all traps.

Modes

Global configuration mode

Usage Guidelines

Regardless of the port the Brocade device uses to send traps to the receiver, the traps always arrive from the same source IP address.

The **no** form of the command removes the configured interface as SNMP trap generator.

Examples

The following example shows how to configure an Ethernet interface as SNMP trap generator source.

```
device(config)# snmp-server trap-source ethernet 1/1/1
```

The following example shows how to configure a loopback interface as SNMP trap generator source.

```
device(config)# snmp-server trap-source loopback 1
```

snmp-server user

Creates or changes the attributes of SNMPv3 users, and allows an SNMPv3 user to be associated with the user-defined group name.

Syntax

snmp-server user *user-name group-name* **v3** [**access** *acl-num*] [**auth** { **md5** | **sha** } *auth-password* [**priv** { **aes** | **des** } *password-string*]]

no snmp-server user *user-name group-name* **v3** [**access** *acl-num*] [**auth** { **md5** | **sha** } *auth-password* [**priv** { **aes** | **des** } *password-string*]]

Command Default

SNMP users are not configured.

Parameters

user-name
Specifies the SNMP username or security name used to access the management module.

group-name
Identifies the SNMP group to which this user is associated or mapped.

v3
Configures the group using the User Security Model (SNMPv3).

access
Specifies the access list associated with the user.

acl-num
Standard IP access list number allowing access. The valid values are from 1 through 99.

auth
Specifies the type of encryption the user must have to be authenticated.

md5
Configures the HMAC MD5 algorithm for authentication.

sha
Configures the HMAC SHA algorithm for authentication.

auth-password
Specifies the authorization password for the user (8 through 16 characters for MD5; 8 through 20 characters for SHA).

priv
Configures the encryption type (DES or AES) used to encrypt the privacy password.

aes
Configures CFB128-AES-128 encryption for privacy.

des
Configures CBC56-DES encryption for privacy.

password-string

Specifies the DES or AES password string for SNMPv3 encryption for the user. The password must have a minimum of 8 characters.

Modes

Global configuration mode

Usage Guidelines

The **snmp-server user** command creates an SNMP user, defines the group to which the user will be associated, defines the type of authentication to be used for SNMP access by this user, specifies either the **AES** or **DES** encryption types used to encrypt the privacy password.

All users must be mapped to an SNMP group. Groups are defined using the **snmp-server group** command.

NOTE
The SNMP group to which the user account will be mapped should be configured before creating the user accounts; otherwise, the group will be created without any views. Also, ACL groups must be configured before configuring user accounts.

NOTE
The ACL specified in a user account overrides the ACL assigned to the group to which the user is mapped. If no ACL is entered for the user account, then the ACL configured for the group will be used to filter packets.

The **priv** parameter specifies the encryption type **(DES or AES)** used to encrypt the privacy password. If the encrypted keyword is used, do the following:

- If **DES** is the privacy protocol to be used, enter **des** followed by a 16-octet DES key in hexadecimal format for the DES-password-key . If you include the encrypted keyword, enter a password string of at least 8 characters.
- If **AES** is the privacy protocol to be used, enter **aes** followed by the AES password key. For a small password key, enter 12 characters. For a big password key, enter 16 characters.

The **no** form of the command removes the SNMP access.

Examples

The following example configures an SNMP user account.

```
device(config)# snmp-server user user1 admin v3 access 2 auth md5 abc123 priv des xyz123
```

snmp-server view

Creates an SNMP view.

Syntax

snmp-server view *view-name mib-subtree* { **excluded** | **included** }

no snmp-server view *view-name mib-subtree* { **excluded** | **included** }

Command Default

All MIB objects are automatically excluded from any view unless they are explicitly included.

Parameters

view-name

Configures the alphanumeric name to identify the view. The names cannot contain spaces.

mib-subtree

Configures the name of the MIB object or family. You can use a wildcard (*) in the numbers to specify a sub-tree family.

excluded

Configures the MIB family identified to be excluded from the view.

included

Configures the MIB family identified to be included in the view.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the configured SNMP view.

SNMP views are named groups of MIB objects that can be associated with user accounts to allow limited access for viewing and modification of SNMP statistics and system configuration. SNMP views can also be used with other commands that take SNMP views as an argument.

MIB objects and MIB sub-trees can be identified by a name or by the numbers called object identifiers (OIDs) that represent the position of the object or sub-tree in the MIB hierarchy.

NOTE
All MIB objects are automatically excluded from any view unless they are explicitly included; therefore, when creating views using the **snmp-server view** command, indicate which portion of the MIB you want users to access.

Examples

The following example assigns the view called "admin" a community string or user group. The "admin" view allows access to the Brocade MIB objects that begin with the 1.3.6.1.4.1.1991 object identifier.

```
device(config)# snmp-server view admin 1.3.6.1.4.1.1991 included
```

source-interface

Configures source IP address of the NTP packets.

Syntax

source-interface { **ethernet** *stackid/slot/port* | **loopback** *num* | **ve** *num* }

no source-interface { **ethernet** *stackid/slot/port* | **loopback** *num* | **ve** *num* }

Command Default

When the system sends an NTP packet, the source IP address is normally set to the address of the lowest IP address of the interface through which the NTP packet is sent.

Parameters

ethernet *stackid/slot/port*

Configures the source IP address for an NTP packet that of the specified Ethernet interface.

loopback *num*

Configures the source IP address for an NTP packet that of the specified loopback interface.

ve *num*

Configures the source IP address for an NTP packet that of the specified Virtual Ethernet interface.

Modes

NTP configuration mode

Usage Guidelines

The specified interface will be used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **peer** or **server** command.

NOTE
If the source-interface is not configured, then the lowest IP address in the outgoing interface will be used in the NTP packets.

The **no** form of the command resets the source IP address of the NTP packets as the IP address of the interface through which it is sent.

Examples

The following example shows how to configure the source IP address for an NTP packet as that of the specified Ethernet interface.

```
device(config)# ntp
device(config-ntp)# source-interface ethernet 1/1/3
```

spanning-tree

Configures STP on all ports on a device.

Syntax

spanning-tree [**single**] [**forward-delay** *seconds*] [**hello-time** *seconds*] [**max-age** *seconds*] [**priority** *number*]

no spanning-tree [**single**] [**forward-delay** *seconds*] [**hello-time** *seconds*] [**max-age** *seconds*] [**priority** *number*]

Command Default

STP is not enabled. Once STP is enabled, the STP port parameters are preconfigured with default values.

Parameters

single
Enables Single STP.

forward-delay *seconds*
Configures the time period a port waits before it forwards an RST BPDU after a topology change. This value ranges from 4 through 30 seconds. The default is 15 seconds.

hello-time *seconds*
Configures the time interval between two Hello packets. This value ranges from 1 through 10 seconds. The default is 2 seconds.

max-age *seconds*
Configures the time period the device waits to receive a Hello packet before it initiates a topology change. The time period ranges from 6 through 40 seconds. The default is 20 seconds.

priority *number*
Configures the priority of the bridge. The value ranges from 0 through 65535. A lower numerical value means the bridge has a higher priority. Thus, the highest priority is 0. The default is 32768.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

You can specify some or all of the parameters on the same command line.

The **single** option which configures a Single STP is available only in the global configuration mode.

The value of **max-age** must be greater than the value of **forward-delay** to ensure that the downstream bridges do not age out faster than the upstream bridges (those bridges that are closer to the root bridge).

Configuring the STP parameters is optional. All parameters have default values. Additionally, all values will be globally applied to all ports on the system or on the port-based VLAN for which they are defined.

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

Examples

The following example configures a Single STP.

```
device(config)# spanning-tree single
```

The following example configures the STP parameters.

```
device(config)# vlan 200
device(config-vlan-200)# spanning-tree forward-delay 4 hello-time 5 max-age 4 priority 20
```

spanning-tree 802-1w

Configures the 802.1w parameters.

Syntax

spanning-tree 802-1w [**single**] [**force-version** *number*] [**forward-delay** *seconds*] [**hello-time** *seconds*] [**max-age** *seconds*] [**priority** *number*]

no spanning-tree 802-1w [**single**] [**force-version** *number*] [**forward-delay** *seconds*] [**hello-time** *seconds*] [**max-age** *seconds*] [**priority** *number*]

Interface configuration mode

spanning-tree 802-1w { **admin-edge-port** | **admin-pt2pt-mac**}

no spanning-tree 802-1w { **admin-edge-port** | **admin-pt2pt-mac**}

Command Default

The 802.1w port parameters are preconfigured with default values.

Parameters

single

Configures Single STP.

force-version *number*

Forces the bridge to send BPDUs in a specific format. 0 for STP compatibility mode and 2 for RSTP default mode.

forward-delay *seconds*

Configures the time period a port waits before it forwards an RST BPDU after a topology change. This value ranges from 4 through 30 seconds. The default is 15 seconds.

hello-time *seconds*

Configures the time interval between two Hello packets. This value ranges from 1 through 10 seconds. The default is 2 seconds.

max-age *seconds*

Configures the time period the device waits to receive a Hello packet before it initiates a topology change. The time period ranges from 6 through 40 seconds. The default is 20 seconds.

priority *number*

Configures the priority of the bridge. The value ranges from 0 through 65535. A lower numerical value means the bridge has a higher priority. Thus, the highest priority is 0. The default is 32768.

admin-edge-port

Configures the port to be an operational edge port for all VLANs.

admin-pt2pt-mac

Configures the port to be on a point-to-point link link for all VLANs.

Modes

Global configuration mode

VLAN configuration mode

Interface configuration mode

Usage Guidelines

The value of **max-age** must be greater than the value of **forward-delay** to ensure that the downstream bridges do not age out faster than the upstream bridges (those bridges that are closer to the root bridge).

Configuring the STP parameters is optional. All parameters have default values. Additionally, all values will be globally applied to all ports on the system or on the port-based VLAN for which they are defined.

The **no** form of the command sets the parameters to the default values.

Examples

The following example shows how to configure the 802.1w parameters.

```
device(config)# vlan 200
device(config-vlan-200)# spanning-tree 802-1w force-version 6 forward-delay 5 hello-time 4 max-age 4
priority 5
```

spanning-tree 802-1w ethernet

Enables the spanning-tree 802.1w port commands on Ethernet ports.

Syntax

spanning-tree 802-1w [**single**] **ethernet** *stackid/slot/port* [**admin-edge-port**] [**admin-pt2pt-mac**] [**force-migration-check**] [**path-cost** *number*] [**priority** *number*] [**disable**]

no spanning-tree 802-1w [**single**] **ethernet** *stackid/slot/port* [**admin-edge-port**] [**admin-pt2pt-mac**] [**force-migration-check**] [**path-cost** *number*] [**priority** *number*] [**disable**]

Command Default

The 802.1w port parameters are pre-configured with default values.

Parameters

single
Configures a Single STP.

ethernet *stackid/slot/port*
Specifies the Ethernet port on which you want to configure the 802.1w parameters.

admin-edge-port
Enables the port as an edge port in the domain.

admin-pt2pt-mac
Enables a port that is connected to another port through a point-to-point link. The point-to-point link increases the speed of convergence. This parameter, however, does not auto-detect whether or not the link is a physical point-to-point link.

force-migration-check
Forces the specified port to sent one RST BPDU. If only STP BPDUs are received in response to the send RST BPDU, then the port will return to sending STP BPDUs.

path-cost *number*
Configures the cost of the port path to the root bridge. 802.1w prefers the path with the lowest cost. The path cost ranges is from 1 through 20,000,000.

priority *number*
Sets the priority for the port. The priority value ranges from 0 through 240, in increments of 16. The default value is 128.

disable
Disables 802.1w for the interface on the VLAN.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

Configuring the parameters is optional. All parameters have default values. Additionally, all values will be globally applied to all ports on the system or on the port-based VLAN for which they are defined.

The **no** form of the command disables the spanning tree on a VLAN

Examples

The following example shows the spanning tree configuration for the specified Ethernet port.

```
device(config)# vlan 200
device(config-vlan-200)# spanning-tree 802-1w ethernet 1/1/3 admin-edge-port admin-pt2pt-mac force-
migration-check path-cost 5 priority 10
```

spanning-tree ethernet

Configures the path and priority costs for a port.

Syntax

spanning-tree [**single**] **ethernet** *stackid/slot/port* { **disable** | **path-cost** { *number* | **auto** } | **priority** *number* }

no spanning-tree [**single**] **ethernet** *stackid/slot/port* { **disable** | **path-cost** { *number* | **auto** } | **priority** *number* }

Command Default

The Ethernet port parameters are preconfigured with default values.

Parameters

single
Configures a Single STP.

disable
Disables STP for the interface on the VLAN.

path-cost *number*
Configures the cost of the port path to the root bridge. STP prefers the path with the lowest cost. The range is from 0 through 65535.

auto
Configures the cost of the port path to be the value set by the system software.

priority *number*
Sets the priority for the port. The priority value ranges from 0 through 240, in increments of 16. The default value is 128.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

The **single** keyword is available only in global configuration mode.

Configuring STP parameter values is optional. All parameters have default values. Additionally, all values will be globally applied to all ports on the system or on the port-based VLAN for which they are defined.

The default path cost depends on the port type:

- 10 Mbps - 100
- 100 Mbps - 19
- 1 Gbps - 4
- 10 Gbps - 2

The **no** form of the command disables the STP on the Ethernet port.

Examples

The following example shows how to configure the path cost and priority for an Ethernet port.

```
device(config)# vlan 10
device(config-vlan-10)# spanning-tree ethernet 1/1/5 path-cost 15 priority 64
```

spanning-tree designated-protect

Disallows the designated forwarding state on a port in STP 802.1d or 802.1w.

Syntax

spanning-tree designated-protect

no spanning-tree designated-protect

Command Default

STP (802.1d or 802.1w) can put a port into designated forwarding state.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command allows the designated forwarding state on a port in STP 802.1d or 802.1w. If STP tries to put a port into designated forwarding state, the device puts this port into the designated inconsistent STP state. This is effectively equivalent to the listening state in STP in which a port cannot forward any user traffic. When STP no longer marks this port as a designated port, the port is automatically removed from the designated inconsistent state.

NOTE
You use this command to enable Designated Protection at the port-level while the designated inconsistent state is a per-STP-instance, per-port state.

NOTE
You cannot enable Designated Protection and Root Guard on the same port.

Examples

The following example disallows the designated forwarding state on interface 1/1/1.

```
device(config)# ethernet interface 1/1/1
device(config-if-e1000-1/1/1)# spanning-tree designated-protect
```

History

Release version	Command history
07.3.00g	This command was introduced.

spanning-tree root-protect

Configures STP root guard.

Syntax

spanning-tree root-protect

no spanning-tree root-protect

Command Default

Root guard is disabled by default.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables STP root guard.

Examples

The following example shows how to enable RSTP on a port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# spanning-tree root-protect
```

spanning-tree rstp

Enables 802.1w Draft 3 in a port-based VLAN.

Syntax

spanning-tree [**single**] **rstp**

no spanning-tree [**single**] **rstp**

Command Default

RSTP is disabled by default.

Parameters

single

Configures single RSTP on the device.

Modes

Global configuration mode

VLAN configuration mode

Usage Guidelines

You must enter the command separately in each port-based VLAN in which you want to run 802.1w Draft 3.

This command does not enable STP. To enable STP, first enter the **spanning-tree** command without the **rstp** parameter. After you enable STP, enter the **spanning-tree rstp** command to enable 802.1w Draft 3.

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

Examples

The following example shows how to enable RSTP on a port.

```
device(config)# vlan 10
device(config-vlan-10)# spanning-tree rstp
```

speed-duplex

Sets link speed and mode (full or half duplex, or slave or master).

Syntax

speed-duplex { **10-full** | **10-half** | **100-full** | **100-half** | **1000-full** | **1000-full-master** | **1000-full-slave** | **10g-full** | | **10g-full-master** | **10g-full-slave** | **2500-full** | **2500-full-master** | **2500-full-slave** | **auto** }

no speed-duplex

Command Default

By default, the speed is auto-negotiated.

Parameters

10-full
10M, full duplex

10-half
10M, half duplex

100-full
100M, full duplex

100-half
100M, half duplex

1000-full
1G, full duplex

1000-full-master
1G, full duplex, master

1000-full-slave
1G, full duplex, slave

10g-full
10G, full duplex

10g-full-master
10G, full duplex, master

10g-full-slave
10G, full duplex, slave

2500-full
2.5G, full duplex

2500-full-master
2.5G, full duplex, master

2500-full-slave
2.5G, full duplex, slave

auto

Auto-negotiation. This is the default.

Modes

Interface configuration mode

Usage Guidelines

The Gigabit Ethernet copper ports are designed to auto-sense and auto-negotiate the speed and duplex mode of the connected device. If the attached device does not support this operation, you can manually enter the port speed to operate at either 10, 100, or 1000 Mbps. The default and recommended setting is 10/100/1000 auto-sense.

On FastIron devices, when setting the speed and duplex-mode of an interface to 1000-full, configure one side of the link as master (1000-full-master) and the other side as slave (1000-full-slave).

Both ends of the link must be configured to operate at the same speed.

The 1000-full setting mode is not applicable to 1G copper ports on the ICX 7250 and ICX 7450 when they are running FastIron software version 8.0.30g (SPR08030g .bin).

On the ICX 7450-32ZP 2.5G ports, this command works in port pairs only. The port speed for the following ports should be changed together: 25-26, 27-28, 29-30, and 31-32.

On the ICX 7750-48C, support for 100-full link speed was added.

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

Examples

The following example changes the port speed of copper interface 1/1/8 on a device from the default of 10/100/1000 auto-sense, to 100 Mbps operating in full-duplex mode.

```
device(config)# interface ethernet 1/1/8
device(config-if-e1000-1/1/8)# speed-duplex 100-full
```

History

Release version	Command history
8.0.20	This command was introduced.
8.0.30g	This command was modified to specify that he 1000-full setting mode is not applicable to 1G copper ports on the ICX 7250 and ICX 7450.
8.0.40	This command was modified to specify that on the ICX 7450-32ZP 2.5G ports, the command works in port pairs only.
8.0.40a	This command was modified to add support for 100M full-duplex mode on the ICX 7750-48C.

ssh

Starts an SSH2 client connection to an SSH2 server using password authentication.

Syntax

ssh { *hostname* | *ipv4-address* } [**public-key** { **dsa** | **rsa** }] [*port-num*]

ssh ipv6 { *hostname* | *ipv6-address* } [**public-key** { **dsa** | **rsa** }] [**outgoing-interface** *type number*] [*port-num*]

Command Default

SSH2 client connection is not established.

Parameters

hostname
: Specifies the host name of the SSH server.

ipv4-address
: Specifies the IPv4 address of the SSH server.

public-key
: Configures the type of public key authentication to use for the connection. If you do not enter this parameter, the default authentication type is password.

dsa
: Specifies the public key authentication type as DSA.

rsa
: Specifies the public key authentication type as RSA.

port-num
: Specifies that the SSH2 connection will use a non-default SSH2 port. The default is 22.

ipv6
: Identifies the remote IPv6 SSH server.

ipv6-address
: Specifies the IPv6 address of the SSH server.

outgoing-interface
: Configures the outgoing interface for Link-Local address.

type
: Specifies the interface type.

number
: Specifies the interface number. Use **?** to get the list of supported interfaces.

Modes

Privileged EXEC mode

Examples

The following example starts an SSH2 client connection to an SSH2 server using password authentication.

```
device# ssh 192.168.10.1
```

The following example starts an SSH2 client connection to an SSH2 server using public key authentication.

```
device# ssh ipv6 2001::1 public-key dsa
```

The following example starts an SSH2 client connection to an SSH2 server using public key authentication.

```
device# ssh ipv6 2001::1 public-key dsa outgoing-interface ethernet 1/1/1 26
```

ssh access-group

Configures an ACL that restricts SSH access to the device.

Syntax

ssh access-group { *acl-num* | *acl-name* | **ipv6** *ipv6-acl-name* }

no ssh access-group { *acl-num* | *acl-name* | **ipv6** *ipv6-acl-name* }

Command Default

SSH access is not restricted.

Parameters

acl-num
: The standard access list number. The valid values are from 1 through 99.

acl-name
: The standard access list name.

ipv6 *ipv6-acl-name*
: The IPv6 access list name.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the SSH access restriction.

Examples

The following example shows how to configure an ACL that restricts SSH access to the device. In this example, ACL 10 is configured. The device allows SSH access to all IP addresses except those listed in ACL 10.

```
device(config)# access-list 10 permit host 10.168.144.241
device(config)# access-list 10 deny host 10.168.144.242 log
device(config)# access-list 10 permit host 10.168.144.243
device(config)# access-list 10 deny any
device(config)# ssh access-group 10
```

stack disable

Prevents a device from joining a traditional stack and from listening for, or sending, stacking packets.

Syntax

stack disable

no stack disable

Command Default

Stacking is disabled by default.

Modes

Global configuration mode and Stack unit configuration mode

Usage Guidelines

To remove the restriction that prevents the unit from joining a stack, use the **no stack disable** command.

Examples

The following example disables the device from joining a stack.

```
device# configure terminal
device(config)# stack disable
Disable stacking. This unit will not be a part of any stack
```

History

Release version	Command history
08.0.00a	This command was introduced.

stack enable

Enables stack configuration on the device. Enter this command on the intended active controller.

Syntax

stack enable

no stack enable

Command Default

Stacking is not enabled on the device.

Modes

Global configuration mode

Stack unit configuration mode

Usage Guidelines

Use the **no** form of the command to remove stacking capability from the device.

> **NOTE**
> When you use the **no stack enable** command, the unit can still be called to join an active stack. To prevent this, use the **stack disable** command instead.
> You must remove all configuration information from the port before issuing the **stack enable** command.

For manual configuration, the **stack enable** command must be issued on each device in the stack.

Examples

The following example enables stack configuration on the device.

```
device# config terminal
device(config)# stack enable
Enable stacking. This unit actively participates in stacking
```

History

Release version	Command history
08.0.00a	This command was introduced.

stack mac

Manually configures a specific MAC address for a traditional stack.

Syntax

stack mac *mac-address*

no stack mac *mac-address*

Command Default

Beginning with FastIron release 08.0.20, when a stack is enabled or when hitless-failover occurs, a default stack MAC address is assigned if none is configured. In earlier releases, the stack assumed the MAC address of the active controller by default.

Parameters

mac-address

Specifies the MAC address to be used for the stack.

Modes

Active stack controller configuration mode

Usage Guidelines

Enter the **no** form of this command to revert to the use of the active controllers' MAC address.

The MAC address is a hexadecimal value entered in the format xxxx.xxxx.xxxx.

Examples

The following example configures the stack MAC address manually as 0000.0000.0011.

```
device(config)# stack mac 0000.0000.0011
device(config)# show running-config
Current configuration:
!
ver 05.0.01 100T7e1
!
stack 1
module 1 fcx-48-port-copper-base-module
module 2 fcx-cx4-1-port-10g-module
priority 80
stack 2
module 1 fcx-24-port-copper-base-module
module 2 fcx-cx4-1-port-10g-module
module 3 fcx-cx4-1-port-10g-module
stack enable
stack mac 0000.0000.0011
```

History

Release version	Command history
08.0.00a	This command was introduced.
08.0.20	Stack behavior was modified so that a default MAC address is assigned when the stack is enabled or when hitless failover occurs if no stack MAC address has been configured.

stack-port

Selects only one of the two stacking ports as a stacking port, which allows you to use the other port as a data port.

Syntax

stack-port *unit/slot/port*

no stack-port

Command Default

By default, both default ports serve as stacking ports on an FCX or ICX stack unit.

Parameters

unit
: Stack unit ID

slot
: Slot or module on the unit where the interface resides.

port
: Interface to be configured as the sole stack port on the unit.

Modes

Stack-unit configuration mode.

Usage Guidelines

The **no** form of the command restores both default stacking ports on the device.

The **stack-port** command should not be used on a live stack.

Examples

The following example configures Port 3/2/1 as the only stacking port on stack unit 3.

```
device# configure terminal
device(config)# stack unit 3
device(config-unit-3)# stack-port 3/2/1
Set only one stacking port 3/2/1
```

stack secure-setup

Configures a stack automatically, to add units to an existing traditional stack, or to change stack member IDs.

Syntax

stack secure-setup

Modes

Privileged EXEC mode of a stack unit

Usage Guidelines

Stacking must be enabled with the **stack enable** command before the **stack secure-setup** command can be issued.

When the **stack secure-setup** command is issued on a unit that is not already the active controller, the unit becomes the active controller.

Examples

In the following example, an FCX traditional stack is formed using **stack secure-setup**.

```
device# stack secure-setup
device# Discovering the stack topology...
Current Discovered Topology - RING
Available UPSTREAM units
Hop(s) Type MAC Address
1 FCX624 0000.0039.2d40
2 FCX624 0000.00d5.2100
Available DOWNSTREAM units
Hop(s) Type MAC Address
1 FCX624 0000.00d5.2100
2 FCX624 0000.0039.2d40
Do you accept the topology (RING) (y/n)?: y
Selected Topology:
Active Id Type MAC Address
1 FCX648 0000.00ab.cd00
Selected UPSTREAM units
Hop(s) Id Type MAC Address
1 3 FCX624 0000.0039.2d40
2 2 FCX624 0000.00d5.2100
Selected DOWNSTREAM units
Hop(s) Id Type MAC Address
1 2 FCX624 0000.00d5.2100
2 3 FCX624 0000.0039.2d40
Do you accept the unit ids (y/n)?: y
```

stack stack-port-resiliency

Configures different levels of corrective steps that an active controller can take to fix stacking ports that cannot send or receive packets, despite the ports being logically operational.

Syntax

stack stack-port-resiliency *level*

no stack stack-port-resiliency *level*

Command Default

The stack-port-resiliency feature is enabled with the *level* variable value set to 1.

Parameters

level

The value determines the corrective steps that an active controller can take when a stack port is malfunctioning. Then value can range from 0 through 3.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the **stack stack-port-resiliency** command sets the *level* variable value to 1.

The **stack stack-port-resiliency** command is only supported on an ICX 6610 in a stack.

The corrective steps that can be taken depend on the value of the *level* variable and involve error-disabling malfunctioning ports or reloading one or more stack units. Traffic may be disrupted for a few seconds or longer while the port malfunction is detected and fixed.

If the *level* value is set to 1 and the unit with the malfunctioning port is not an active controller:

- The active controller checks whether other ports in the same static LAG are fully operational.
- If the total bandwidth of the operational static LAG is greater than or equal to 20 Gbps, the malfunctioning port is error-disabled.
- If the total bandwidth of the operational static LAG is less than 20 Gbps and error-disabling all ports of the LAG could disconnect one or more other units from the stack, the unit reloads.
- If the total bandwidth of the operational static LAG is less than 20 Gbps and error-disabling all ports of the LAG would not disconnect any other units from the stack, all the ports of the LAG are error-disabled.

If the *level* value is set to 2 and the unit with the malfunctioning port is not the active controller, the unit reloads. After the reload, if any other non-active controller unit is not able to communicate with the active controller, it also reloads.

If the *level* value is set to 3, the corrective steps in level 2 are performed. If the port is still not operating correctly, the entire stack reloads.

If you use the command and set the *level* variable value to 1, this configuration shows in the **show run** command output. If you use the **no** form of the command, the *level* variable value is set to 1, but the value does not show in the **show run** command output.

NOTE
You can use the **show errdisable summary** command to view a list of all error-disabled ports, along with the reason the ports were error-disabled.

Examples

The following example shows the configuration of stack port resiliency on a stack with the *level* variable value set to 2.

```
Device# configure terminal
Device(config)# stack stack-port-resiliency 2
```

History

Release version	Command history
07.3.00g	This command was introduced.

stack suggested-id

Specifies the preferred stack unit ID for a standalone device before it joins a stack.

Syntax

stack suggested-id *stack-unit*

no stack suggested-id *stack-unit*

Parameters

stack-unit

Specifies the numeric stack unit ID.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command removes the stack unit ID.

The **stack suggested-id** command is configured on a standalone device before it joins a stack and becomes a member. The command is not for the active controller. Because the active controller always keeps its bootup ID during stack formation, it does not use the suggested-id value.

The system attempts to assign a bootup ID of a device as its stack unit ID. However, due to timing issues or the possible unavailability of the bootup ID, a device might not get the stack unit ID that you want when the stack is formed. The optional **stack suggested-id** command allows you to specify the stack unit ID for member devices when you are configuring a traditional or mixed stack using the manual configuration method.

Examples

The following example sets the stack unit ID on a standalone device to 3.

```
device# configure terminal
device(config)# stack suggested-id 3
```

stack suppress-warning

Stops periodic output of background stack diagnostic reports.

Syntax

stack suppress-warning

no stack suppress-warning

Command Default

By default, background diagnostics are displayed periodically on the active stack controller.

Modes

Stack active controller configuration mode

Usage Guidelines

Use the **no** form of the command to restore periodic output of background diagnostic reports.

Examples

In the following example, background diagnostic reports are turned off for the stack.

```
Device# configure terminal
Device(config)# stack suppress-warning
```

stack switch-over

Switches active controllers without reloading the stack and without packet loss to services and protocols supported by hitless stacking.

Syntax

stack switch-over

Command Default

With FastIron release 08.0.20, the **stack switch-over** command is allowed by default. In earlier releases, hitless failover must first be enabled.

Modes

Global configuration mode on a stack controller

Usage Guidelines

Use the **stack switch-over** command before reloading or performing maintenance on the currently active controller. Hitless failover must be enabled for the command to be used; otherwise, an error message is issued.

The command cannot be used during stack election or during configuration of a multi-stack-trunk.

A standby controller must exist and must have learned stack protocols for the command to be used. The standby controller must have the same priority as the active controller for the command to be used.

More than 120 seconds must have passed since the previous switchover or failover for the command to be accepted.

Examples

The following example shows the **stack switch-over** command being entered and the resulting output. You must confirm the switch-over before it can take effect by entering **y** when prompted.

```
device# stack switch-over
Standby unit 8 will become active controller, and unit 1 will become standby
Are you sure? (enter 'y' or 'n'): y
Unit 1 is no longer the active controller
```

History

Release version	Command history
08.0.00a	This command was introduced.
08.0.20	Hitless failover is enabled by default. The **stack switch-over** command is allowed by default as a result.

stack-trunk

Configures a stack to form a trunk from contiguous links on one side of a stack connection.

Syntax

stack-trunk *stack-unit/slotnum/portnum* **to** *stack-unit/slotnum/portnum*

no stack-trunk *stack-unit/slotnum/portnum* **to** *stack-unit/slotnum/portnum*

Parameters

stack-unit
: Specifies the stack unit ID.

slotnum
: Specifies the slot number.

portnum
: Specifies the port number in the slot.

Modes

Stack unit configuration mode

Usage Guidelines

Use the **no** form of the command to disable the stack trunk configuration.

The **stack-trunk** command must be configured on the stack units on both ends of the trunk. Use this command in a new environment on the first deployment of a stack.

To enable the **stack-trunk** command, the primary port in the trunk must be configured under the **stack-port** command configuration.

Do not use the **stack-trunk** command in a production environment. Use the **multi-stack-trunk** command instead.

Examples

In the following example, ports 1/2/3 and 1/2/4 are configured as a stacking trunk on stack unit 1.

```
Device# configure terminal
Device(config)# stack unit 1
Device(config-unit-1)# stack-trunk 1/2/3 to 1/2/4
```

stack unconfigure

Returns a stack member to its pre-stacking configuration or state.

Syntax

stack unconfigure [**stack-unit** | **all** | **me** | **clean** | **mixed-stack**]

Parameters

stack-unit

Specifies the numerical ID of a stack member. This option is available on the active controller only.

all

Specifies all stack members. This option is available on the active controller only.

me

Specifies the stack member from which the command is executed. The command removes the unit from the stack and boots it up as a standalone. When the unit rejoins the stack, its standalone startup-config file is saved in a backup file. This option is available on stack member consoles only.

clean

Specifies that the startup configuration be removed from the unit on which the command is executed and that the unit be rebooted as a clean unit. This option is available on stack member consoles only.

mixed-stack

Specifies removal of all peripheral ports and peripheral trunks from ICX 6610 devices. It also specifies recovery and reload of prior ICX 6450 peripheral device configurations, from before the ICX 6450 units were members of the mixed stack. This option is available only on the active controller in a mixed stack.

Modes

Privileged EXEC mode

Usage Guidelines

When a stack unit that did not have an original startup configuration file is unconfigured, it becomes a clean unit. It is possible that this unit could automatically rejoin the stack if its module configuration matches the configuration of the active controller. To prevent this from happening accidentally, disconnect the unit to be unconfigured, and then issue the **stack unconfigure me** command on it.

Examples

Examples

In the following example, stack unit 2 is unconfigured in a traditional stack.

```
Device(config)# show stack
alone: standalone, D: dynamic config, S: static config
ID  Typ    Role    Mac Address    Pri State  Comment
1 S FCX624 active  0012.f2eb.a900 128 local  Ready
2 S FCX648 standby 00f0.424f.4243 0   remote Ready
3 S FCX624 member  00e0.5201.0100 0   remote Ready

Device# stack unconfigure 2
Will recover pre-stacking startup config of this unit, and reset it. Are you sure?
(enter 'y' or 'n'): y

Stack 2 deletes stack bootup flash and recover startup-config.txt from .old

Device# show stack
alone: standalone, D: dynamic config, S: static config
ID  Type   Role    Mac Address    Pri State   Comment
1 S FCX624 active  0012.f2eb.a900 128 local   Ready
2 S FCX648 member  0000.0000.0000 0   reserved
3 S FCX624 standby 00e0.5201.0100 0   remote  Ready
```

Examples

In the following example, ICX 6450 peripheral devices are removed from a mixed stack. The mixed stack contains two ICX 6610 devices in a ring configuration in the backbone. There are two sub-stacks of three ICX 6450 devices each in the mixed stack.

The following **show stack** output shows the configuration of the mixed stack before the stack **unconfigure mixed-stack** command is executed. The **show stack** command is executed on the active controller.

```
Brocade(config)# show stack
alone: standalone, D: dynamic config, S: static config
ID  Typ    Role    Mac Address    Pri State  Comment
1 S FCX624 active  0012.f2eb.a900 128 local  Ready
2 S FCX648 standby 00f0.424f.4243 0   remote Ready
3 S FCX624 member  00e0.5201.0100 0   remote Ready

Brocade# stack unconfigure 2
Will recover pre-stacking startup config of this unit, and reset it. Are you sure?
(enter 'y' or 'n'): y

Stack 2 deletes stack bootup flash and recover startup-config.txt from .old

Brocade# show stack
alone: standalone, D: dynamic config, S: static config
ID  Type   Role    Mac Address    Pri State   Comment
1 S FCX624 active  0012.f2eb.a900 128 local   Ready
2 S FCX648 member  0000.0000.0000 0   reserved
3 S FCX624 standby 00e0.5201.0100 0   remote  Ready

    active       standby
     +---+        +---+
 =2/6| 1 |2/1==2/6| 2 |2/1=
  |   +---+        +---+   |
  |                        |
  |------------------------|

    active                                              standby
      ---         +---+        +---+        +---+         ---
     ( 1 )3/7--2/1| 6 |2/3==2/1| 7 |2/3==2/1| 8 |2/3==3/7( 2 )
      ---         +---+        +---+        +---+         ---

    standby                                             active
      ---         +---+        +---+        +---+         ---
     ( 2 )3/1==2/1| 5 |2/3==2/1| 4 |2/3==2/1| 3 |2/3--3/1( 1 )
      ---         +---+        +---+        +---+         ---
```

The following sequence shows the **stack unconfigure mixed-stack** command being executed on the active controller. After confirmation, all peripheral ports and peripheral trunks are removed from the ICX 6610 units. The peripheral ICX 6450 devices recover their configurations from before they were members of the mixed stack, and they are reloaded.

```
Brocade# stack unconfigure mixed-stack
All the peri-ports/trunks will be removed and all the ICX6450 units will recover
pre-mixed-stacking configuration. Are you sure? (enter 'y' or 'n'): y
Removed peri-ports from configuration:  1/3/1 1/3/7
Removed peri-trunks from configuration: 2/3/1-to-2/3/2 2/3/7-to-2/3/8
```

The **show stack** command is executed on the active controller. The output shows that the ICX 6450 devices are no longer part of the mixed stack because the MAC addresses are all zeroes, the State column shows “reserve,” and the device status in the Comment column does not show “Ready.”

The Role column still shows “member” because the active controller holds the configuration of the former stack member in reserve so that it can form a stack later if a stack is merged or formed.

```
Brocade# show stack
alone: standalone, D: dynamic config, S: static config
ID   Type         Role    Mac Address    Pri State   Comment
1  S ICX6610-24F  active  748e.f891.c5b8 128 local   Ready
2  S ICX6610-48P  standby 748e.f834.4d14   0 remote  Ready
```

```
3  S ICX6450-24   member  0000.0000.0000   0 reserve
4  S ICX6450-24P  member  0000.0000.0000   0 reserve
5  S ICX6450-24P  member  0000.0000.0000   0 reserve
6  S ICX6450-48   member  0000.0000.0000   0 reserve
7  S ICX6450-48   member  0000.0000.0000   0 reserve
8  S ICX6450-24P  member  0000.0000.0000   0 reserve

    active       standby
     +---+        +---+
 =2/6| 1 |2/1==2/6| 2 |2/1=
  |   +---+        +---+   |
  |                        |
  |------------------------|
```

Use the **show stack** command to verify that peripheral devices, such as ICX 6450 devices, are no longer part of the mixed stack.

In the following example, the Role column shows “alone,” which indicates a standalone device. This means that the device was a standalone device before joining the mixed stack.

```
Brocade# show stack

***** Warning! stack is not enabled. *****

alone: standalone, D: dynamic config, S: static config
ID   Type         Role    Mac Address    Pri State   Comment
1  S ICX6450-24P  alone   748e.f8b0.6c00   0 local   None:0


     +---+
  2/1| 1 |2/3
     +---+
Current stack management MAC is 748e.f8b0.6c00
Note: no "stack mac" config. My MAC will change after failover.
```

In the following example, the Role column shows “active,” “standby,” or “member,” which indicates that these devices are part of a stack. This means that the devices were part of a traditional stack before joining the mixed stack.

```
Brocade# show stack
alone: standalone, D: dynamic config, S: static config
ID   Type         Role    Mac Address    Pri State   Comment
1  S ICX6450-24P  active  748e.f8b0.6c00 128 local   Ready
2  S ICX6450-48   standby 748e.f8d4.2300   0 remote  Ready
3  S ICX6450-48   member  748e.f8d4.02c0   0 remote  Ready

                 standby      active
     +---+        +---+        +---+
  2/1| 3 |2/3--2/1| 2 |2/3--2/1| 1 |2/3
     +---+        +---+        +---+
Standby u2 - No hitless failover. Reason: hitless-failover not configured
Current stack management MAC is 748e.f8b0.6c00
Note: no "stack mac" config. My MAC will change after failover.
```

History

Release	Command History
07.4.00	This command was introduced.
08.0.00a	The **mixed-stack** option was added. The **rollback** option was deprecated.

static ethernet

Enables a static protocol VLAN membership.

Syntax

static ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no static ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

A static protocol VLAN membership is not configured.

Parameters

stackid/slot/port
Specifies the Ethernet port on which the static protocol VLAN membership is to be enabled.

to *stackid/slot/port*
Specifies the range of ports on which the static protocol VLAN membership is to be enabled.

Modes

IP protocol VLAN configuration mode

IPX protocol VLAN configuration mode

IPv6 protocol VLAN configuration mode

AppleTalk protocol VLAN configuration mode

DECnet protocol VLAN configuration mode

NetBIOS protocol VLAN configuration mode

Other protocol VLAN configuration mode

IP subnet VLAN configuration mode

Usage Guidelines

The **no** form of the command disables the static protocol VLAN membership.

Examples

The following example shows how to enable static protocol VLAN membership.

```
device (config)# vlan 3
device(config-vlan-3)# ip-subnet 10.1.2.0/24 name Yellow
device(config-vlan-ip-subnet)# no dynamic
device(config-vlan-ip-subnet)# static ethernet 1/1/9 to 1/1/16 ethernet 1/1/25
```

static-mac-address

Configures a static MAC address and assigns the address to the premium queue.

Syntax

static-mac-address *ethernet-mac-address* **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...] [**priority** *number*]

no static-mac-address *ethernet-mac-address* **ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...] [**priority** *number*]

static-mac-address *ethernet-mac-address* **drop**

no static-mac-address *ethernet-mac-address* **drop**

Command Default

By default, all MAC addresses are in the best-effort queue.

Parameters

ethernet-mac-address
Specifies the MAC address of the Ethernet interface.

ethernet *stackid/slot/port*
Specifies the Ethernet interface.

to
Specifies the range of the Ethernet ports.

priority *number*
Configures a priority to the Ethernet MAC address. The values are from 0 through 7.

drop
Drop the packets to and from the specified Ethernet MAC address.

Modes

Global configuration mode (in case of a single VLAN)

VLAN configuration mode (in case of multiple VLANs)

Usage Guidelines

The **no** form of the command clears the static MAC address configuration.

Examples

The following example configures a static MAC address on a range of Ethernet interfaces with priority 7.

```
device(config)# static-mac-address 0000.0063.67ff ethernet 1/1/1 to 1/1/6 priority 7
```

The following example configures a VLAN to drop packets with a source or destination MAC address.

```
device(config)# vlan 2
device(config-vlan-2)# static-mac-address 0000.0063.67FF drop
```

static-mac-ip-mapping

Adds the client MAC address mapping to the IP address.

Syntax

static-mac-ip-mapping *ip-address mac-address*

no static-mac-ip-mapping *ip-address mac-address*

Parameters

ip-address

Specifies the IP address of the client to be used for mapping.

mac-address

Specifies the MAC address of the client to be used for mapping.

Modes

DHCP server pool configuration mode

Usage Guidelines

The **no** form of the command removes the client MAC address mapping from the IP address.

Examples

The following example adds the client MAC address mapping to the IP address.

```
device# configure terminal
device(config)# ip dhcp-server pool cabo
device(config-dhcp-cabo)# static-mac-ip-mapping 10.10.10.29 0010.9400.0005
```

History

Release version	Command history
08.0.30mb	This command was introduced.

store-and-forward

Resets the switching method for forwarding packets from cut-through to store-and-forward.

Syntax

store-and-forward

no store-and-forward

Command Default

The switching method is cut-through.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command restores the default packet-forwarding method to cut-through.

Ethernet devices support two basic switching methods for packet forwarding: store-and-forward and cut-through. The default method on ICX 7750 devices is cut-through. You can configure the **store-and forward** command to change it to store-and-forward.

NOTE
You must save the configuration and reload for the change to take effect.

A store-and-forward device does not make a forwarding decision on a data packet until it has received the whole frame and checked its integrity; a cut-through device starts the forwarding process soon after it makes the forwarding decision on an incoming frame that is, it might start forwarding before the entire packet is received. This reduces forwarding latency, especially for longer packets. However, there are many factors to consider when selecting which switching method is best for your environment and in some cases it is desirable to change from the default method and configure a device to store-and-forward.

The following table describes some of the differences in how packets are handled depending on the switching method.

Feature	Cut-through	Store-and-forward
Forwarding	Data forwarding starts before an entire packet is received	Device waits for entire packet received before processing.
Latency	Low latency, less than 1 micro second.	Higher latency; latency depends on frame size.
FCS Errors	FCS errors may be propagated from one device to another.	FCS errors are checked and error packets are discarded in the MAC receive.
MTU size	MTU size is validated by MAC receive. Oversize packets are marked as error packets but not dropped in the MAC receive.	MTU size is validated by MAC receive. Oversize packets are dropped at the MAC layer.

Examples

This example globally enables **store-and-forward** packet switching and saves the configuration.

```
Device(config)# store-and-forward
Device(config)# write memory
Device(config)# end
```

History

Release version	Command history
08.0.10b	This command was introduced.

stp-bpdu-guard

Enables STP BPDU Guard on the Ethernet interfaces.

Syntax

stp-bpdu-guard

no stp-bpdu-guard

Command Default

STP BPDU Guard is disabled by default.

Modes

Interface configuration mode

Usage Guidelines

When a BPDU Guard-enabled port is disabled by BPDU Guard, the Brocade device places the port in the errdisable state and displays a message on the console indicating that the port is errdisabled.

The **no** form of the command disables the STP BPDU Guard on the Ethernet interfaces.

Examples

The following example shows how to enable the STP BPDU Guard on a port.

```
device(config)# interface ethernet 1/2/1
device(config-if-e1000-1/2/1)# stp-bpdu-guard
```

The following example shows how to enable the STP BPDU Guard on multiple ports.

```
device(config)# interface ethernet 1/1/1 to 1/1/9
device(config-mif-1/1/1-1/1/9)# stp-bpdu-guard
```

stp-group

Changes the CLI to the STP group configuration level.

Syntax

stp-group *group-id*

no stp-group *group-id*

Parameters

group-id

Specifies the STP group ID. The value ranges from 1 through 32.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command exits the STP group configuration level.

Examples

The following example shows how to change to the STP group configuration level.

```
device(config)# stp-group 1
device(config-stp-group-1)#
```

stp-protect

Prevents an end station from initiating or participating in STP topology changes.

Syntax

stp-protect

no stp-protect

Command Default

STP protection is disabled by default.

Modes

Interface configuration mode

Usage Guidelines

This command causes the port to drop STP BPDUs sent from the device on the other end of the link.

The **no** form of the command disables STP protection on the port.

Examples

The following example shows how to enable STP protection on a port.

```
device(config)# interface ethernet 1/1/2
device#(config-if-e1000-1/1/2)# stp-protect
```

supptimeout

Configures the amount of time the Brocade device should wait for the client to respond to the Extensible Authentication Protocol (EAP)-request/identity frame before retransmitting the EAP-request/identity frame to the client.

Syntax

supptimeout *seconds*

no supptimeout *seconds*

Command Default

The default value is 30 seconds.

Parameters

seconds

Specifies the amount of time the Brocade device should wait for the client to respond to the EAP-request/identity frame before retransmitting the EAP-request/identity frame to the client. The value range is from 1 through 4294967295 seconds.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command resets the default time of 30 seconds for the Brocade device to wait for the client to respond to the EAP-request/identity frame before retransmitting the EAP-request/identity frame.

Examples

The following example configures the device to retransmit the EAP-request/identity frame if the client does not respond within 45 seconds.

```
device(config)# dot1x-enable
device(config-dot1x)# supptimeout 45
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

switch-over-active-role

Activates switchover of the active and standby management modules without any packet loss to the services and protocols that are supported by Hitless management.

Syntax

switch-over-active-role

Command Default

Switch over is not enabled.

Modes

Privileged EXEC mode

Usage Guidelines

Hitless failover must be enabled before a hitless switchover can be executed.

If this command is entered when hitless failover is disabled, the following message will appear on the console:

```
Switch-over is not allowed. Reason: hitless-failover not configured.
```

NOTE
Command supported only on FSX devices.

Examples

The following example shows how to switch over to the standby module.

```
device# switch-over-active-role
Are you sure? (enter 'y' or 'n'): y
Running Config data has been changed. Do you want to continue
the switch-over without saving the running config? (enter 'y' or 'n'): n
Please save the running config and try switch-over again
```

symmetrical-flow-control enable

Enables symmetrical flow control (SFC) globally for priorities.

Syntax

symmetrical-flow-control enable [**all**]

no symmetrical-flow-control enable

Command Default

SFC is globally disabled.

Parameters

all

Specifies SFC on all priorities. If you do not specify the **all** keyword, SFC is enabled only on priorities 0-4. This parameter is optional.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this restores the default flow-control settings.

Configuring the **symmetrical-flow-control enable** command enables SFC globally for priorities 0-4 by default and optionally for all priorities (0-7)

By default, the system runs in tail-drop mode, with all ports honoring 802.3x flow control and disabling 802.3x transmit. The **symmetrical-flow-control enable** command enables transmission of 802.3x pause frames.

Configuring the **symmetrical-flow-control enable** command changes priority-to-PG mapping.

You cannot configure the **symmetrical-flow-control enable** command if the **priority-flow-control** command is enabled.

If the **symmetrical-flow-control enable** command is not enabled, you cannot configure the **flow-control generate-only** or the **flow-control both** commands in interface configuration mode.

NOTE
In FastIron Release 08.0.20 and later releases, SFC is not supported for ports across stack units in ICX 7750 devices or across stack units or for ports across master and slave packet-processor (pp) devices in ICX7450-48 units.

Examples

The following example shows how to enable SFC:

```
Device(config)# symmetrical-flow-control enable
```

The following example shows how to enable all priorities to send the IEEE 802.3x pause:

```
Device(config)# symmetrical-flow-control enable all
```

The following example shows how to enable SFC for Generate-only mode:

```
Device(config)# symmetrical-flow-control enable
Device(config)# flow-control generate-only
```

The following example shows how to enable SFC for both Honor and Generate-only mode:

```
Device(config)# symmetrical-flow-control enable
Device(config)# flow-control both
```

History

Release version	Command history
8.0.10	This command was introduced.

symmetric-flow-control enable

Enables symmetric flow control globally on all full-duplex data ports of a standalone unit or on all full-duplex data ports of a particular unit in a traditional stack.

Syntax

symmetric-flow-control enable [**unit** *stack-unit* [*stack-unit*] ...]

no symmetric-flow-control enable [**unit** *stack-unit* [*stack-unit*] ...]

Command Default

Symmetric flow control is disabled and tail drop mode is enabled.

Parameters

unit *stack-unit*

Specifies one of the units in a stacking system for which symmetric flow control has to be enabled. You can specify up to 8 units.

Modes

Global configuration mode

Usage Guidelines

As flow control is enabled by default on all full-duplex ports, these ports will always honor received 802.3x Pause frames, whether or not symmetric flow control is enabled.

The **no** form of the command disables symmetric flow control.

Examples

The following example shows how to enable symmetric flow control globally on all full-duplex data ports of a standalone unit.

```
device(config)# symmetric-flow-control enable
```

The following example shows how to enable symmetric flow control globally on all full-duplex data ports of a particular unit in a traditional stack.

```
device(config)# symmetric-flow-control enable unit 4
```

symmetric-flow-control set

Sets symmetric flow control parameters.

Syntax

symmetric-flow-control set *port-type* { **buffers** *value* [**unit** *unit-value*] | **xoff** *num* **xon** *num* }

no symmetric-flow-control set *port-type* { **buffers** *value* [**unit** *unit-value*] | **xoff** *num* **xon** *num* }

Command Default

Defaults: 1G : Buffers: 272, XOFF Limit: 91, XON Limit: 75

10G: Buffers: 416, XOFF Limit: 91, XON Limit: 75

Parameters

port-type

Specifies the port type. The port type can be one of the following

1

Sets the buffer limits or XOFF and XON limits for 1G ports.

2

Sets the buffer limits or XOFF and XON limits for 10G ports.

3

Sets the buffer limits or XOFF and XON limits for 100G ports.

buffers *value*

Sets the total buffer limits. The value can range from 64 to 320 for 1G ports and 64 to 1632 for 10G ports. The default value for 1G ports is 272 and 416 for 10G ports.

unit *unit-value*

Specifies the buffer limit for a stack unit.

xoff *num*

Sets the XOFF limit. The minimum value is 60% and the maximum value is 95%.

xon *num*

Sets the XON limit. The minimum value is 50% and the maximum value is 90%.

Modes

Global configuration mode

Usage Guidelines

Use the **show symmetric** command to view the default or configured buffer limit or XON and XOFF thresholds.

The **no** form of the command deletes the configured symmetric flow control values.

Examples

The following example shows how to change the thresholds for all 1G ports.

```
device(config)# symmetric-flow-control set 1 xoff 91 xon 75
```

The following example shows how to change the total buffer limit for all 10G ports.

```
device(config)# symmetric-flow-control set 2 buffers 128
Total buffers modified, 1G: 320, 10G: 128
```

system-max hw-traffic-conditioner

Configures the maximum number of traffic policies supported on a Layer 3 device.

Syntax

system-max hw-traffic-conditioner *num*

Command Default

The default is 992.

Parameters

num

Specifies the maximum number of active traffic policies. Value is 992.

Modes

Global configuration mode

Examples

The following example shows how to set the maximum number of active traffic policies to 992.

```
device(config)# system-max hw-traffic-conditioner 992
```

system-max igmp-snoop-group-addr

Sets the maximum number of IGMP group addresses on a device.

Syntax

system-max igmp-snoop-group-addr *num*

no system-max igmp-snoop-group-addr

Command Default

The default number of IGMP group addresses is supported.

Parameters

num

Specifies the maximum number of IGMP group addresses supported. The range is a value from 256 through 8192. The default for IGMP snooping group addresses is 4096, except for ICX 6430 devices where the default is 1024.

Modes

Global configuration mode

Usage Guidelines

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

The configured number of IGMP group addresses is the upper limit of an expandable database. Client memberships exceeding the group limit are not processed.

The following describes the IGMP group address limits for Brocade devices:

- FCX, FSX, ICX 6610, and ICX 6450 devices support up to 8192 IGMP group addresses.
- ICX 6430 devices support up to 4096 IGMP group addresses.
- ICX 6650 devices support 8192 IGMP group addresses.
- ICX 7750 switches support 8192 IGMP group addresses.
- ICX 7750 routers support 6K IGMP group addresses.
- ICX 7250 devices support 8192 IGMP group addresses.
- ICX 7450 devices support 8192 IGMP group addresses.

Examples

This example sets maximum number of IGMP snooping group addresses to 1600.

```
Device(config)#system-max igmp-snoop-group-addr 1600
```

system-max igmp-snoop-mcache

Configures the maximum number of IGMP snooping cache entries supported on a device.

Syntax

system-max igmp-snoop-mcache *num*

no system-max igmp-snoop-mcache

Command Default

The default number of IGMP snooping cache entries is supported.

Parameters

num

Specifies the maximum number of IGMP snooping cache entries supported. The range is a value from 256 through 8192. The default is 512 entries except on ICX 6430 devices, where the default is 256.

Modes

Global configuration mode

Usage Guidelines

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

The following describes the IGMP snooping multicast cache (mcache) resource limits for Brocade devices:

- FCX, FSX, ICX 6610, and ICX 6450 devices support up to 8192 IGMP snooping mcache entries.
- ICX 6430 devices support up to 2048 IGMP snooping mcache entries.
- ICX 6650 devices support 8192 IGMP snooping mcache entries.
- ICX 7750 switches support 8192 IGMP snooping mcache entries.
- ICX 7750 routers support 6K IGMP snooping mcache entries.
- ICX 7250 devices support 8192 IGMP snooping mcache entries.
- ICX 7450 devices support 8192 IGMP snooping mcache entries.

Examples

This example shows how to configure the maximum number of IGMP snooping mcache entries supported on the device to 2000.

```
Device(config)#system-max igmp-snoop-mcache 2000
```

system-max ip-route

Increases the capacity of the IP route table.

Syntax

system-max ip-route *number*

no system-max ip-route *number*

Command Default

The default is 12000 for FCX, ICX 6450, and ICX 6610 devices. The default is 262144 for FSX devices. The default is 5120 for ICX 6650 devices.

Parameters

number

The maximum number of routes in the IP route table.

Modes

Global configuration mode

Usage Guidelines

The supported ranges and defaults for IP routes vary by platform:

Product	Default number of IP routes	**Supported range**
FCX	12000	4096 to 15168
ICX 6610	12000	4096 to 15168
FSX	262144	4096 to 524288
ICX 6450	12000	4096 to 12000
ICX 6650	5120	2048 to 7168

You must save the configuration and reload the software to place the system maximum change into effect.

The **no** form of the command resets the values to the default.

Examples

The following example increases the capacity of the IP route table:

```
device(config)# system-max ip-route 5000
device(config)# write memory
device(config)# exit
device# reload
```

system-max ip-subnet-port

Increases the number of IP subnet interfaces that can be configured on each port of the device.

Syntax

system-max ip-subnet-port *number*

no system-max ip-subnet-port *number*

Command Default

The default number of IP subnet interfaces is 24.

Parameters

number

Specifies the maximum number of IP subnets per port. The range is from 24 through 128. The default value is 24.

Modes

Global configuration mode

Usage Guidelines

You must save the configuration and reload the software to place the system maximum change into effect.

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

Examples

The following example increases the capacity of the IP subnet interfaces.

```
device(config)# system-max ip-subnet-port 64
device(config)# write memory
device(config)# exit
device# reload
```

system-max mac

Changes the capacity of the MAC address table.

Syntax

system-max mac *number*

no system-max mac *number*

Command Default

The default capacity is 65536 MAC addresses.

Parameters

number

The maximum number of MAC addresses in the MAC table. The valid range is from 32768 through 65536. The default value is 65536.

Modes

Global configuration mode

Usage Guidelines

This command is supported only on ICX 6650, and you can change the capacity of the MAC address table. By default, up to 65536 MAC addresses are supported.

On FSX and ICX 6450 devices, the supported value is 16384. On FCX devices, the supported value is 32768. You cannot change these values.

You must save the configuration and reload the software to place the system maximum change into effect.

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

Examples

The following example increases the capacity of the MAC address table.

```
device(config)# system-max mac 32768
device(config)# write memory
device(config)# exit
device# reload
```

system-max mac-notification-buffer

Changes the value of the MAC-notification buffer.

Syntax

system-max mac-notification-buffer *size*

no system-max mac-notification-buffer *size*

Command Default

The default buffer size is 4000.

Parameters

size Sets the buffer queue size to maintain MAC-notification events.

Modes

Global configuration

Usage Guidelines

The **no** form of the command sets the MAC-notification buffer to default size. The default buffer value is 4000, maximum value is 16000, and the allowed values are 4000, 8000 and 16000.

Examples

This example changes the value of the MAC-notification buffer:

```
device(config)# system-max mac-notification-buffer 8000
```

This example sets the MAC-notification buffer to default size:

```
device(config)# no system-max mac-notification-buffer 4000
```

History

Release version	Command history
08.0.10	This command was introduced.

system-max max-ecmp

Configures the maximum limit of ECMP paths at the system level.

Syntax

system-max max-ecmp [*num*]

no system-max max-ecmp [*num*]

Command Default

The default value is 8.

Parameters

num

Specifies the maximum number of ECMP paths and can be from 8 through 32.

Modes

Global configuration mode

Usage Guidelines

The **system-max max-ecmp** command is supported only on the Brocade ICX 7750.

If the maximum number of ECMP paths is not configured at the system level, by default, you can configure the maximum number of IP load sharing paths to a value from 2 through 8.

The configuration of the maximum number of IP load sharing paths to a value more than 8 is determined by the maximum number of ECMP paths configured at the system level using the **system-max max-ecmp** command.

You cannot configure the maximum number of IP load sharing paths higher than the value defined at the system level.

You cannot configure the maximum number of ECMP paths at the system level to a value less than the configured IP load sharing value.

You must save the configuration and reload the device for the maximum ECMP value change to take effect.

The **no** form of the command removes the maximum number of ECMP paths defined at the system level.

Examples

The following example defines the maximum number of ECMP paths that can be configured in the system as 20.

```
device(config)# system-max max-ecmp 20
device(config)# write memory
device(config)# exit
device# reload
```

History

Release version	Command history
08.0.30	This command was introduced.

system-max mld-snoop-group-addr

Sets the maximum number of multicast listening discovery (MLD) group addresses on a device.

Syntax

system-max mld-snoop-group-addr *num*

no system-max mld-snoop-group-addr

Command Default

The default number of MLD group addresses is supported.

Parameters

num

Specifies the maximum number of MLD group addresses supported. The range is a value from 256 through 8192. The default for MLD snooping group addresses is 4096, except for ICX 6430 devices where the default is 1024.

Modes

Global configuration mode

Usage Guidelines

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

The configured number of MLD group addresses is the upper limit of an expandable database. Client memberships exceeding the group limit are not processed.

The following describes the MLD group address limits for Brocade devices:

- FCX, FSX, ICX 6610, and ICX 6450 devices support up to 8192 MLD group addresses.
- ICX 6430 devices support up to 4096 MLD group addresses.
- ICX 6650 devices support 8192 MLD group addresses.
- ICX 7750 switches support 8192 MLD group addresses.
- ICX 7750 routers support 6K MLD group addresses.
- ICX 7250 devices support 8192 MLD group addresses.
- ICX 7450 devices support 8192 MLD group addresses.

Examples

This example sets maximum number of MLD snooping group addresses to 4000.

```
Device(config)#system-max mld-snoop-group-addr 4000
```

system-max mld-snoop-mcache

Configures the maximum number of multicast listening discovery (MLD) snooping cache entries supported on a device.

Syntax

system-max mld-snoop-mcache *num*

no system-max mld-snoop-mcache

Command Default

The default number of MLD snooping cache entries is supported.

Parameters

num

Specifies the maximum number of MLD snooping cache entries supported. The range is 256 to 8192. The default is 512 entries except on ICX 6430 devices, where the default is 256.

Modes

Global configuration mode

Usage Guidelines

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

The following describes the MLD snooping multicast cache (mcache) resource limits for Brocade devices:

- FCX and FSX devices support up to 8192 MLD snooping mcache entries.
- ICX 6610, ICX 6450, and ICX 6650 devices support up to 8192 MLD snooping mcache entries.
- ICX 7250 and ICX 7450 devices support up to 8192 MLD snooping mcache entries.
- ICX 7750 switches support up to 8192 MLD snooping mcache entries.
- ICX 6430 devices support up to 2048 MLD snooping mcache entries.
- ICX 7750 routers support 3072 MLD snooping mcache entries.
- In Release 8.0.10a and later releases, ICX 7750 routers support 6144 MLD snooping mcache entries.

Examples

This example shows how to set the maximum number of MLD snooping mcache entries to 8000.

```
Device(config)#system-max mld-snoop-mcache 8000
```

system-max openflow-flow-entries

Configures the openflow flow table entries limit in the flow table.

Syntax

system-max openflow-flow-entries *number*

Command Default

The system-max openflow-flow-entries is enabled. The default value is 3072 flow table entries.

Parameters

number

Specifies a value from 0 to 12288.

Modes

Global configuration mode

Examples

The following example configures openflow flow table entries limit in the flow table.

```
device# configure terminal
device(config)# system-max openflow-flow-entries 304
```

History

Release	Command History
08.0.30	This command was introduced.

system-max openflow-pvlan-entries

Configures the CAM size of openflow protected VLAN entries for the device.

Syntax

system-max openflow-pvlan-entries *number*

Command Default

The system-max openflow-pvlan-entries is enabled. The default value is 40.

Parameters

number

Specifies a value from 0 to 40.

Modes

Global configuration mode

Examples

The following example configures system-max openflow-pvlan-entries

```
device# configure terminal
device(config)# system-max openflow-pvlan-entries 30
```

History

Release	Command History
08.0.30	This command was introduced.

system-max openflow-unprotectedvlan-entries

Configures the CAM size of openflow unprotected VLAN entries for the device.

Syntax

system-max openflow-unprotectedvlan-entries *number*

Command Default

The system-max openflow-unprotectedvlan-entries is enabled. The default value is 40.

Parameters

number

Specifies a value from 0 to 40.

Modes

Global configuration mode

Examples

The following example configures system-max openflow-unprotected-entries

```
device# configure terminal
device(config)# system-max openflow-unprotectedvlan-entries 30
```

History

Release	Command History
08.0.30	This command was introduced.

system-max rmon-entries

Configures the maximum number of entries allowed in the RMON control table.

Syntax

system-max rmon-entries *value*

no system-max rmon-entries *value*

Command Default

The default number of RMON entries allowed in the RMON control table is 1024. The default number of RMON entries allowed in the RMON control table is 2048 on the FSX device.

Parameters

value

Specifies the number of entries. The value can range from 128 to 32768. The value can range from 1536 to 32768 for FSX devices.

Modes

Global configuration mode

Usage Guidelines

This command configures the maximum number of entries allowed in the RMON control table, including alarms, history, and events.

NOTE
You must save the change to the startup-config file and reload or reboot. The change does not take effect until you reload or reboot.

The **no** form of the command resets the maximum number of entries allowed in the RMON table to the default value.

Examples

The following example shows how to set the number of RMON entries to 3000.

```
device(config)# system-max rmon-entries 3000
device(config)# write mem
device(config)# exit
device# reload
```

system-max spanning-tree

Configures the system maximum value for the number of spanning tree instances.

Syntax

system-max spanning-tree *number*

no system-max spanning-tree *number*

Command Default

The default number of spanning tree instances is 32.

Parameters

number

Configures the number of spanning tree instances. The range is from 1 through 254.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the system maximum value of spanning tree instances to the default.

Examples

The following example shows how to set the maximum number of spanning tree instances.

```
device(config)# system-max spanning-tree 254
```

system-max view

Configures the number of SNMP views available on a device.

Syntax

system-max view *number-of-views*

no system-max view *number-of-views*

Command Default

The default number of views is 10.

Parameters

number-of-views

Specifies the maximum number of SNMPv2 and SNMPv3 views. The number of views can range from 10 to 65535. The default value is 10.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the number of views to the default value 10.

Examples

The following example configures the number of SNMP views as 15.

```
device(config)# system-max view 15
```

system-max virtual-interface

Increases the maximum number of virtual routing interfaces you can configure.

Syntax

system-max virtual-interface *num*

no system-max virtual-interface *num*

Command Default

The default maximum number of virtual interfaces that can be configured is 255.

Parameters

num

Specifies the maximum number of the virtual routing interface that can be configured. The range depends on the device being configured.

Modes

Global configuration mode

Usage Guidelines

The number of virtual routing interfaces supported on your product depends on the device and, for chassis devices, the amount of DRAM on the management module. The **write memory** command must be executed to save the changes and a reload is required.

The **no** form of the command removes the configured maximum number of virtual routing interfaces and resets the maximum value to the default.

Examples

The following example shows how to increase the maximum number of virtual routing interfaces.

```
device(config)# system-max virtual-interface 512
device(config)# write memory
device(config)# end
device# reload
```

system-max vlan

Increases the maximum number of VLANs you can configure.

Syntax

system-max vlan *num*

no system-max vlan *num*

Command Default

The default maximum value is 64 VLANs.

Parameters

num

Specifies the maximum number of VLANs you can configure. The range depends on the device being configured.

Modes

Global configuration mode

Usage Guidelines

Although you can specify up to 4095 VLANs, you can configure only 4094 VLANs. VLAN ID 4094 is reserved for use by Single STP. The **write memory** command must be executed to save the changes and a reload is required. The number of VLANs supported on your product depends on the device and, for chassis devices, the amount of DRAM on the management module.

The **no** form of the command removes the maximum number of VLANs and resets the maximum value to 64.

Examples

The following example shows how to increase the maximum number of VLANs.

```
device(config)# system-max vlan 2048
device(config)# write memory
device(config)# end
device# reload
```

tacacs-server deadtime

Configures the duration for which the device waits for the primary authentication server to reply before deciding the TACACS server is dead and trying to authenticate using the next server.

Syntax

tacacs-server deadtime *time*

no tacacs-server deadtime *time*

Command Default

The default duration is three seconds.

Parameters

time

The time in seconds. The valid values are from 1 through 5. The default is 3.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the duration for which the device waits for a reply before deciding that the server is dead.

Examples

The following example configures the dead time as four seconds.

```
device(config)# tacacs-server deadtime 4
```

tacacs-server enable

Configures the device to allow TACACS server management access only to clients connected to ports within port-based VLAN.

Syntax

tacacs-server enable vlan *vlan-number*

no tacacs-server enable vlan *vlan-number*

Command Default

By default, access is allowed on all ports.

Parameters

vlan *vlan-number*

Configures access only to clients connected to ports within the VLAN.

Modes

Global configuration mode

Usage Guidelines

You can restrict management access to a Brocade device to ports within a specific port-based VLAN. VLAN-based access control works in conjunction with other access control methods. Clients connected to ports that are not in the VLAN are denied management access.

The **no** form of the command removes the restriction.

Examples

The following example shows how to allow TACACS server access only to clients in a specific VLAN.

```
device(config)# tacacs-server enable vlan 10
```

tacacs-server host

Configures the TACACS server host to authenticate access to a Brocade device.

Syntax

tacacs-server host { *ipv4-address* | *host-name* | *ipv6-address*} [**auth-port** *port-num* [**acct-port** *port-num* [{ **accounting-only** | **authentication-only** | **authorization-only** | **default** } [**key** *key-string*]]]

no tacacs-server host { *ipv4-address* | *host-name* | *ipv6-address*} [**auth-port** *port-num* [**acct-port** *port-num* [{ **accounting-only** | **authentication-only** | **authorization-only** | **default** } [**key** *key-string*]]]

Command Default

The TACACS server host is not configured.

Parameters

ipv4-address
Configures the IPv4 address of the TACACS server.

host-name
Configures the host name of the TACACS server.

ipv6-address
Configures the IPv6 address of the TACACS 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. Supported for TACACS+ only.

authentication-only
Configures the server to be used only for authentication. Supported for TACACS+ only.

authorization-only
Configures the server to be used only for authorization. Supported for TACACS+ only.

default
Configures the server to be used for any AAA operation. Supported for TACACS+ only.

key *key-string*
Configures the TACACS key for the server. Supported for TACACS+ only.

Modes

Global configuration mode

Usage Guidelines

You can specify up to eight servers. If you add multiple TACACS or TACACS+ authentication servers to the Brocade device, the device tries to reach them in the order you add them. To use a TACACS server to authenticate access to a Brocade device, you must identify the server to the Brocade device. In a TACACS configuration, you can designate a server to handle a specific AAA task. For example, you can designate one TACACS server to handle authorization and another TACACS server to handle accounting. You can specify individual servers for authentication and accounting, and authorization. You can set the TACACS key for each server.

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

Examples

The following example shows how to configure a TACACS server to authenticate access to a Brocade device.

```
device(config)# tacacs-server host 192.168.10.1
```

The following example shows how to specify different TACACS servers for authentication and accounting.

```
device(config)# tacacs-server host 10.2.3.4 auth-port 1800 acct-port 1850 default key abc
device(config)# tacacs-server host 10.2.3.5 auth-port 1800 acct-port 1850 authentication-only key def
device(config)# tacacs-server host 10.2.3.6 auth-port 1800 acct-port 1850 accounting-only key ghi
```

tacacs-server key

Configures the value that the Brocade device sends to the TACACS server when trying to authenticate user access.

Syntax

tacacs-server key *key-string*

no tacacs-server key *key-string*

Command Default

The TACACS server key is not configured.

Parameters

key-string

Specifies the key as an ASCII string. The value for the key parameter on the Brocade device should match the one configured on the TACACS server. The key can be from 1 to 32 characters in length and cannot include any space characters.

Modes

Global configuration mode

Usage Guidelines

The **tacacs-server key** command is used to encrypt TACACS packets before they are sent over the network.

The **no** form of the command removes the TACACS server key configuration.

Examples

The following example shows how to configure a TACACS server key.

```
device(config)# racacs-server key abc
```

tacacs-server retransmit

Configures the maximum number of retransmission attempts for a request when a TACACS authentication request times out.

Syntax

tacacs-server retransmit *number*

no tacacs-server retransmit *number*

Command Default

The default number of retries is three.

Parameters

number

The maximum number of retries the Brocade software will retransmit the request. The valid values are from 1 through 5. The default is 3.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command resets the maximum number of retransmission attempts to the default.

Examples

The following example shows how to set the maximum number of retransmission attempts to four.

```
device(config)# tacacs-server retransmission 4
```

tacacs-server timeout

Configures the number of seconds the Brocade device waits for a response from a TACACS server before either retrying the authentication request or determining that the TACACS servers are unavailable and moving on to the next authentication method in the authentication method list.

Syntax

tacacs-server timeout *time*

no tacacs-server timeout *time*

Command Default

The default timeout value is three seconds.

Parameters

time

The time in seconds. Valid values are from 1 through 15 seconds. The default is 3.

Modes

Global configuration mode

Usage Guidelines

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

Examples

The following example shows how to set the TACACS server timeout value to 10 seconds.

```
device(config)# tacacs-server timeout 10
```

tagged ethernet

Tags a port to allow communication among the different VLANs to which the port is assigned.

Syntax

tagged ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]

no tagged ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]

Parameters

ethernet *stackid/slot/port*
Specifies the Ethernet interface to configure as a tagged port.

to *stackid/slot/port*
Specifies a range of Ethernet interfaces.

Modes

VLAN configuration mode

Usage Guidelines

Tagging does not apply to the default VLAN. The ports are defined as either tagged or untagged at the VLAN level.

The **no** form of the command removes the tagging of the Ethernet ports.

Examples

The following example tags the port 1/1/9 to VLAN 4.

```
device(config)# vlan 4
device(config-vlan-4)# tagged ethernet 1/1/9
```

tag-profile

Configures or changes the tag profile for 802.1ad tagging.

Syntax

tag-profile *tag-number*

no tag-profile *tag-number*

Command Default

The default tag number is 0x8100.

Parameters

tag-number

Specifies the number of the tag. The value can be 0x8100 (default) or 0xffff.

Modes

Global configuration mode

Usage Guidelines

Tag profiles on a single port, or a group of ports, can be configured to point to the global tag profile.

The **no** command removes the tag profile configuration.

Examples

The following example shows how to configure the tag profile.

```
device(config)# tag-profile 9500
```

tag-profile enable

Directs the individual ports or a range of ports to the tag profile.

Syntax

tag-profile enable

no tag-profile enable

Command Default

The tag profile is not enabled.

Modes

Interface configuration mode

Usage Guidelines

Tag profiles on a single port, or a group of ports, can be configured to point to the global tag profile.

The tag type and tag profile cannot be configured at the same time.

The **no** form of the command disables the tag profile for ports.

Examples

The following example shows how to enable tag profile for a single port.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# tag-profile enable
```

The following example shows how to enable tag profile for multiple ports.

```
device(config)# interface ethernet 1/1/1 ethernet 1/2/1
device(config-mif-1/1/1,1/2/1)# tag-profile enable
```

tag-type

Enables 802.1ad tagging for aggregated VLANs.

Syntax

tag-type *num* [**ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]]

no tag-type *num* [**ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]]

Command Default

802.1ad tagging is not enabled.

Parameters

num

Specifies the tag type can be a hexadecimal value from 0 - ffff. The default is 8100.

ethernet *stackid/slot/port*

Specifies the ports that will use the defined 802.1Q tag.

to *stackid/slot/port*

Specifies a range of ports that will use the defined 802.1Q tag.

Modes

Global configuration mode

Usage Guidelines

802.1ad tagging provides finer granularity for configuring 802.1Q tagging, enabling you to configure 802.1Q tag types on a group of ports. This command allows you to create two identical 802.1Q tags (802.1ad tagging) on a single device.

To enable 802.1ad tagging, configure an 802.1Q tag on the untagged edge links (the customer ports) to any value other than the 802.1Q tag for incoming traffic.

If you specify a single port number, the 802.1Q tag applies to all ports within the port region. If you do not specify a port or range of ports, the 802.1Q tag applies to all Ethernet ports on the device.

NOTE
Brocade devices treat a double-tagged Ethernet frame as a Layer 2-only frame. The packets are not inspected for Layer 3 and Layer 4 information, and operations are not performed on the packet utilizing Layer 3 or Layer 4 information.

The tag type and tag profile cannot be configured at the same time.

The **no** form of the command removes the tag type configuration.

Examples

The following example shows how to enable the 802.1ad tagging.

```
device(config)# tag-type 9100 ethernet 1/1/11 to 1/1/12
```

telnet access-group

Configures an ACL that restricts Telnet access to the device.

Syntax

telnet access-group { *acl-num* | *acl-name* | **ipv6** *ipv6-acl-name* }

no telnet access-group { *acl-num* | *acl-name* | **ipv6** *ipv6-acl-name* }

Command Default

Telnet access is not restricted.

Parameters

acl-num
: The standard access list number. The valid values are from 1 through 99.

acl-name
: The standard access list name.

ipv6 *ipv6-acl-name*
: The IPv6 access list name.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the Telnet access restriction.

Examples

The following example shows how to configure an ACL that restricts Telnet access to the device. In this example, ACL 10 is configured. The device allows Telnet access to all IP addresses except those listed in ACL 10.

```
device(config)# access-list 10 deny host 10.157.22.32 log
device(config)# access-list 10 deny 10.157.23.0 0.0.0.255 log
device(config)# access-list 10 deny 10.157.24.0 0.0.0.255 log
device(config)# access-list 10 deny 10.157.25.0/24 log
device(config)# access-list 10 permit any
device(config)# telnet access-group 10
device(config)# write memory
```

telnet client

Restricts Telnet access to a host with the specified IP address.

Syntax

telnet client { *ipv4-address* [*client-mac*] | **any** *client-mac* | **ipv6** *ipv6-address*}

no telnet client { *ipv4-address* [*client-mac*] | **any** *client-mac* | **ipv6** *ipv6-address*}

Command Default

Remote Telnet access is not restricted.

Parameters

ipv4-address
: Allows Telnet access only to the host with the IPv4 address.

client-mac
: The host MAC address.

any *client-mac*
: Allows Telnet access to a host with any IP address but with the specified MAC address.

ipv6 *ipv6-address*
: Allows Telnet access to a host with the specified IPv6 address.

Modes

Global configuration mode

Usage Guidelines

You can specify only one IP address with one command. However, you can enter the command ten times to specify up to ten IP addresses.

The **no** form of the command removes the restriction and allows Telnet access to all the clients.

Examples

The following example shows how to allow Telnet access only to the host with IP address 192.168.10.1 and MAC address 1111.2222.3333.

```
device(config)# telnet client 192.168.10.1 1111.2222.3333
```

telnet login-retries

Configures the number of attempts you can enter a correct username and password before the device disconnects the Telnet session.

Syntax

telnet login-retries *number*

no telnet login-retries *number*

Command Default

By default, four attempts are supported.

Parameters

number

The number of retries the device prompts you for a username and password before disconnecting the Telnet session. The valid values are from 0 through 5. The default is 4.

Modes

Global configuration mode

Usage Guidelines

If you are connecting to the Brocade device using Telnet, the device prompts you for a username and password. By default, you have up to four chances to enter a correct username and password. If you do not enter a correct username or password after four attempts, the Brocade device disconnects the Telnet session.

The **no** form of the command resets the number of attempts to the default.

NOTE
You must configure Telnet with the **enable telnet authentication local** command to enable only a specific number of Telnet login attempts.

Examples

The following example shows how to configure up to five chances to enter a correct username and password before getting disconnected.

```
device(config)# telnet login-retries 5
```

telnet login-timeout

Configures the login timeout for a Telnet session.

Syntax

telnet login-timeout *time*

no telnet login-timeout *time*

Command Default

The default login timeout is one minute.

Parameters

time

Time in minutes. The valid values are from 1 through 10. The default is 1.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command sets the login timeout value to the default.

Examples

The following example shows how to set the login timeout value of a Telnet session to ten minutes.

```
device(config)# telnet login-timeout 10
```

telnet server enable

Configures Telnet access only to clients in a specific VLAN.

Syntax

telnet server enable vlan *vlan-num*

no telnet server enable vlan *vlan-num*

Command Default

Telnet access is not restricted.

Parameters

vlan *vlan-num*

Configures access only to clients connected to ports within the VLAN.

Modes

Global configuration mode

Usage Guidelines

You can restrict Telnet access to a Brocade device to ports within a specific port-based VLAN. VLAN-based access control works in conjunction with other access control methods. Clients connected to ports that are not in the VLAN are denied management access.

The **no** form of the command allows Telnet access to all clients.

Examples

The following example shows how to allow Telnet access only to clients connected to ports within port-based VLAN 40.

```
device(config)# telnet server enable vlan 40
```

telnet server suppress-reject-message

Configures the device to suppress the Telnet connection rejection message.

Syntax

telnet server suppress-reject-message

no telnet server suppress-reject-message

Command Default

Rejection messages are sent.

Modes

Global configuration mode

Usage Guidelines

By default, if a Brocade device denies Telnet management access to the device, the software sends a message to the denied Telnet client. You can optionally suppress the rejection message. When you enable the option, a denied Telnet client does not receive a message from the Brocade device. Instead, the denied client simply does not gain access.

The **no** form of the command configures the device to send the rejection message.

Examples

The following example shows the configuration to suppress the connection rejection message sent by the device to a denied Telnet client.

```
device(config)# telnet server suppress-reject-message
```

telnet timeout

Configures the duration of time, a Telnet session can remain idle before it is timed out.

Syntax

telnet timeout *time*

no telnet timeout *time*

Command Default

The Telnet session never times out.

Parameters

time

The time in minutes. The valid values are from 0 through 240. The default is 0; the session never times out.

Modes

Global configuration mode

Usage Guidelines

An idle Telnet session is a session that is still sending TCP ACKs in response to keep alive messages from the device, but is not being used to send data.

The **no** form of the command resets the default timeout value.

Examples

The following example shows how to set the Telnet session idle timeout to 100 minutes.

```
device(config)# telnet timeout 100
```

terminal monitor

Enables the real-time display for a Telnet or SSH session.

Syntax

terminal monitor

Command Default

Real-time display is not enabled.

Modes

Privileged EXEC mode

Usage Guidelines

The command toggles the feature on and off. The CLI displays a message to indicate the status change for the feature. To enable or disable the feature in the management session, enter the **terminal monitor** command again.

Any terminal logged on to a Brocade switch can receive real-time Syslog messages when the **terminal monitor** command is issued.

Examples

The following example shows how to enable real-time display for a Telnet or SSH session.

```
device# terminal monitor
Syslog trace was turned ON
SYSLOG: <9>device, Power supply 2, power supply on left connector, failed
SYSLOG: <14>device, Interface ethernet 6, state down
SYSLOG: <14>device, Interface ethernet 2, state up
```

The following example shows how to disable real-time display for a Telnet or SSH session.

```
device# terminal monitor
Syslog trace was turned OFF
```

tftp client enable

Configures the device to allow TFTP access only to clients in a specific VLAN.

Syntax

tftp client enable vlan *vlan-num*

no tftp client enable vlan *vlan-num*

Command Default

TFTP client access is enabled for all the clients.

Parameters

vlan *vlan-num*

Configures access only to clients connected to ports within the VLAN.

Modes

Global configuration mode

Usage Guidelines

You can restrict TFTP access to a Brocade device to ports within a specific port-based VLAN. VLAN-based access control works in conjunction with other access control methods. Clients connected to ports that are not in the VLAN are denied management access.

The **no** form of the command allows access to all clients.

Examples

The following example shows how to allow TFTP access only to clients connected to ports within port-based VLAN 40.

```
device(config)# tftp client enable vlan 40
```

tftp disable

Disables TFTP client access.

Syntax

tftp disable

no tftp disable

Command Default

TFTP client access is enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command enables TFTP client access.

Examples

The following example shows how to disable TFTP client access.

```
device(config)# tftp disable
```

tftp-server

Specifies the address or name of the TFTP server to be used by the DHCP client.

Syntax

tftp-server { **address** | **name** *server-name* }

Parameters

address

Specifies the IP address of the DHCP server.

name *server-name*

Configures the TFTP server specified by the server name.

Modes

DHCP server pool configuration mode.

Usage Guidelines

If DHCP options 66 (TFTP server name) and option 150 (TFTP server IP address) are both configured, the DHCP client ignores option 150 and tries to resolve the TFTP server name (option 66) using DNS.

Examples

The following example specifies the TFTP server to be used by the DHCP client.

```
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# tftp-server 10.7.5.48
```

table-map

Maps external entry attributes into the BGP routing table, ensuring that those attributes are preserved after being redistributed into OSPF.

Syntax

table-map *string*

no table-map *string*

Command Default

This option is disabled.

Parameters

string

Specifies a route map to be whose attributes are to be preserved. Range is from 1 through 63 ASCII characters.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to remove the table map.

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.

Use this command only to set the tag values. Normally, a route map is applied on routes (and therefore the routes are updated) before it is stored in the BGP routing table. Use the **table-map** command to begin the update before the routes are stored in the IP routing table.

Configurations made by this command apply to all peers.

Route maps that contain **set** statements change values in routes when the routes are accepted by the route map. For inbound route maps (route maps that filter routes received from neighbors), the routes are changed before they enter the BGP4 routing table. For tag values, if you do not want the value to change until a route enters the IP routing table, you can use a table map to change the value. A table map is a route map that you have associated with the IP routing table. The device applies the **set** statements for tag values in the table map to routes before adding them to the routing table. To configure a table map, you first configure the route map, then identify it as a table map. The table map does not require separate configuration. You can have only one table map.

NOTE

Use table maps only for setting the tag value. Do not use table maps to set other attributes. To set other route attributes, use route maps or filters. To create a route map and identify it as a table map, enter commands such those shown in the first example below. These commands create a route map that uses an address filter. For routes that match the IP prefix list filter, the route map changes the tag value to 100 and is then considered as a table map. This route map is applied only to routes that the device places in the IP routing table. The route map is not applied to all routes. The first example below assumes that IP prefix list p11 has already been configured.

Examples

This example illustrates the execution of the **table-map** command.

```
device# configure terminal
device(config)# route-map tag_ip permit 1
device(config-route-map/tag_ip)# match ip address prefix-list p11
device(config-route-map/tag_ip)# set tag 100
device(config-route-map/tag_ip)# exit
device(config-bgp-router)# table-map tag_ip
```

This example removes a table map in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# no table-map tag_ip
```

timers (BGP)

Adjusts the interval at which BGP KEEPALIVE and HOLDTIME messages are sent.

Syntax

timers { **keep-alive** *keepalive_interval* **hold-time** *holdtime_interval* }

no timers

Command Default

The keepalive timer is 60 seconds. The hold timer is 180 seconds.

Parameters

keep-alive *keepalive_interval*

Frequency in seconds with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

hold-time *holdtime_interval*

Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

Modes

BGP configuration mode

Usage Guidelines

Use the **no timers** command to clear the timers.

The KEEPALIVE and HOLDTIME message interval is overwritten when the **fast-external-failover** command takes effect on a down link to a peer.

You must enter a value for **keep-alive** before you can enter a value for **hold-time**. Both values must be entered. If you only want to adjust the value of one parameter, enter the default value of the parameter that you do not want to adjust.

Examples

This example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# timers keep-alive 120 hold-time 360
```

timeout (EFM-OAM)

Configures the time in seconds for which the local Data Terminal Equipment (DTE) waits to receive OAM Protocol Data Units (OAMPDUs) from the remote entity.

Syntax

timeout *value*

no timeout *value*

Command Default

The default value is 5 seconds.

Parameters

value

Specifies the time in seconds for which the local DTE must wait for OAMPDUs from the remote entity. The value range can be from 1 through 10 seconds.

Modes

EFM-OAM protocol configuration mode

Usage Guidelines

If the local DTE does not receive any OAMPDU within the specified period, the peer is considered down and the EFM-OAM discovery process will start over again.

The **no** form of the command restores the default value of 5 seconds.

Examples

The following example configures the timeout value as 10 seconds.

```
device(config)# link-oam
device(config-link-oam)# timeout 10
```

History

Release version	Command history
08.0.30	This command was introduced.

timeout quiet-period

Configures the amount of time the Brocade device waits before retrying to authenticate the client.

Syntax

timeout quiet-period *seconds*

no timeout quiet-period *seconds*

Command Default

The default value is 60 seconds.

Parameters

seconds

Specifies the amount of time the Brocade device waits before retrying to authenticate the client. The value range is from 0 through 4294967295 seconds.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command resets the default time of 60 seconds for the Brocade device to wait before retrying to authenticate the client.

Examples

The following example configures the device to wait for 30 seconds before retrying to authenticate the client.

```
device(config)# dot1x-enable
device(config-dot1x)# timeout quiet-period 30
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

timeout re-authperiod

Changes the re-authentication interval at which the device periodically re-authenticates the clients connected to 802.1X-enabled interfaces.

Syntax

timeout re-authperiod *seconds*

no timeout re-authperiod *seconds*

Command Default

The device re-authenticates the clients connected to 802.1X-enabled interfaces every 3,600 seconds.

Parameters

seconds

Specifies the re-authentication interval at which the device periodically re-authenticates the clients connected to 802.1X-enabled interfaces. The value range is from 1 through 4294967295 seconds.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command resets the re-authentication interval to 3,600 seconds.

Examples

The following example configures periodic re-authentication at an interval of 2,000 seconds.

```
device(config)# dot1x-enable
device(config-dot1x)# re-authentication
device(config-dot1x)# timeout re-authperiod 2000
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

timeout restrict-fwd-period

Configures the amount of time the Brocade device waits for the client to send the non-Extensible Authentication Protocol (EAP) packets before the client is moved to a restricted VLAN.

Syntax

timeout restrict-fwd-period *seconds*

no timeout restrict-fwd-period *seconds*

Command Default

The default value is 10 seconds.

Parameters

seconds

Specifies the amount of time the Brocade device waits for the Client to send the non-EAP packets. The value range is from 0 through 4294967295 seconds.

Modes

dot1x configuration mode

Usage Guidelines

The **no** form of the command resets the default time of 10 seconds for the Brocade device to wait for the client to send the non-EAP packets.

Examples

The following example configures the Brocade device to wait for the client to send the non-EAP packets within 15 seconds before the client is moved to a restricted VLAN.

```
device(config)# dot1x-enable
device(config-dot1x)# restrict-forward-non-dot1x
device(config-dot1x)# timeout restrict-fwd-period 15
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

timeout tx-period

Configures the waiting period for Extensible Authentication Protocol (EAP) frame retransmission.

Syntax

timeout tx-period *time*

no timeout tx-period *time*

Command Default

The default time is 30 seconds.

Parameters

time

Specifies the amount of time the Brocade device waits before retransmitting the EAP-request/identity frame to the client. Valid values are from 1 through 4294967295 seconds. The default value is 30 seconds.

Modes

dot1x configuration mode

Usage Guidelines

If the client does not send back an EAP-response/identity frame within the specified time, the device will transmit another EAP-request/ identity frame.

The **no** form of the command resets waiting period for EAP frame retransmission to the default value.

Examples

The following example configures the device to wait for 60 seconds before retransmitting an EAP-request/ identity frame to a client.

```
device(config)# dot1x-enable
device(config-dot1x)# timeout tx-period 60
```

History

Release version	Command history
08.0.20	This command was removed from Brocade ICX 6430, Brocade ICX 6450, Brocade ICX 6610, Brocade FCX, and Brocade ICX 7750.

topology-group

Configures the topology group.

Syntax

topology-group *group-id*

no topology-group *group-id*

Command Default

A topology group is not configured.

Parameters

group-id

Specifies the topology group ID. The ID ranges from 1 through 256.

Modes

Global configuration mode

Usage Guidelines

Each topology group contains a master VLAN and can contain one or more member VLANs and VLAN groups. You must configure the master VLAN and member VLANs or member VLAN groups before you configure the topology group.

You can configure up to 30 topology groups (On the Brocade ICX 6650, you can configure up to 256 topology groups). Each group can control up to 4096 VLANs. A VLAN cannot be controlled by more than one topology group. The topology group must contain a master VLAN and can also contain individual member VLANs, VLAN groups, or a combination of individual member VLANs and VLAN groups.

The **no** form of the command removes the topology group.

Examples

The following example configures the topology group with ID 2 and adds master VLAN and member VLANs.

```
device(config)# topology-group 2
device(config-topo-group-2)# master-vlan 2
device(config-topo-group-2)# member-vlan 3
device(config-topo-group-2)# member-vlan 4
device(config-topo-group-2)# member-vlan 5
device(config-topo-group-2)# member-group 2
```

traceroute

Determines the path through which a Brocade device can reach another device.

Syntax

traceroute [**vrf** *vrf-name*] *ipv4-address* [**source-ip** *ip-address*] [**minttl** *min-value*] [**maxttl** *max-value*] [**numeric**] [**timeout** *value*]

traceroute *host-name* [**source-ip** *ip-address*] [**minttl** *min-value*] [**maxttl** *max-value*] [**numeric**] [**timeout** *value*]

traceroute ipv6 [**vrf** *vrf-name*] *ipv6-address* [**minttl** *min-value*] [**maxttl** *max-value*] [**numeric**] [**timeout** *value*]

traceroute ipv6 *host-name* [**minttl** *min-value*] [**maxttl** *max-value*] [**numeric**] [**timeout** *value*]

Parameters

vrf *vrf-name*
Specifies the VPN Routing/Forwarding instance.

ipv4-address
Specifies the host IPv4 address.

source-ip *ip-addr*
Configures an IP address to be used as the origin for the traceroute.

minttl *min-value*
Specifies the Minimum TTL (hops) value. The value can range from 1 to 255. Default value is 1 second.

maxttl *max-value*
Specifies the Maximum TTL (hops) value. The value can range from 1 to 255. Default value is 30 seconds.

timeout *value*
Configures echo request timeout. The value can range from 1 to 120. Default value is 2 seconds.

numeric
Configures to display IP addresses in number format instead of their names.

hostname
Specifies the host name.

ipv6
Displays IPv6 related information.

ipv6-address
Specifies the host IPv6 address.

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

The CLI displays trace route information for each hop as soon as the information is received. Traceroute requests display all responses to a given TTL. In addition, if there are multiple equal-cost routes to the destination, the Brocade device displays up to three responses by default.

Examples

The following example shows how to set an IPv4 traceroute.

```
device> traceroute 10.33.4.7
```

The following example shows how to set an IPv6 traceroute.

```
device> traceroute 2001:384d::21:22
```

track-port (VSRP)

Configures the VRID on one interface to track the link state of another interface on the device.

Syntax

track-port { **ethernet** *stackid/slot/port* | **ve** *number* } [**priority** *number*]

no track-port { **ethernet** *stackid/slot/port* | **ve** *number* } [**priority** *number*]

Command Default

The VRID does not track an interface.

Parameters

ethernet *stackid/slot/port*
: Configures the Ethernet interface to track.

ve *number*
: Configures the virtual Ethernet interface to track.

priority *number*
: Changes the VSRP priority of the interface. The range is from 1 through 254.

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.

Command behavior can cause short-path forwarding to be disabled temporarily. As one or more ports tracked by the **track-port** command go down, the current priority of VRRP-E is lowered by a specific amount configured in the **track-port** command for each port. Once the current priority of VRRP-E is lower than the threshold value configured as the revert-priority value, short-path forwarding is temporarily suspended because VRRP-E reverts back to its default forwarding behavior.

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 1/2/4
```

The following example configures the VRID to track a VE interface.

```
device(config)# vlan 200
device(config-vlan-200)# vsrp vrid 1
device(config-vlan-200-vrid-1)# track-port ve 4 priority 4
```

traffic-policy count

Configures a traffic policy and enables counting the number of bytes and the conformance level per packet.

Syntax

traffic-policy *traffic-policy-def* **count**

no traffic-policy *traffic-policy-def* **count**

Command Default

No traffic policy is applied.

Parameters

traffic-policy-def

Specifies the name of the traffic policy definition, in no more than seven alphanumeric characters.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command deletes a traffic policy definition.

Examples

This example configures a traffic policy named TPD and enables counting of bytes and conformance levels.

```
device#configure terminal
device(config)#traffic-policy TPD count
```

traffic-policy rate-limit adaptive

Configures an ACL-based flexible-bandwidth traffic policy to define rate limits on packets so that you can allow for bursts above the limit.

Syntax

traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **count**

traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action drop** [**count**]

traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

no traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **count**

no traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action drop** [**count**]

no traffic-policy *traffic-policy-def* **rate-limit adaptive cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

Command Default

No traffic policy is applied.

Parameters

traffic-policy-def
Specifies the name of the traffic policy definition, in no more than seven alphanumeric characters.

count
Enables counting the number of bytes and the conformance level per packet. The single-rate three-color marker (srTCM) mechanism described in RFC 2697 is used.

cir *cir-value*
Specifies the committed information rate (CIR) in Kbps, that is, the guaranteed rate of inbound traffic that is allowed on a port. The range is 64 through 1,000,000 Kbps. On ICX 6650 devices, the *cir-value* is the rate in packets per second. The range is 125 through 15,000,000 packets per second.

cbs *cbs-value*
Specifies the committed burst size (CBS), that is, the number of bytes per second allowed on a port before some packets exceed the CIR. You must specify a value greater than 0. On ICX 6650 devices, the *cbs-value* is the rate in packets per second.

pir *pir-value*
Specifies the peak information rate (PIR) in Kbps, that is, the most inbound traffic that is allowed on a port. On ICX 6650 devices, the *cir-value* is the rate in packets per second. The *pir-value*must be equal to or greater than the *cir-value*.

pbs *pbs-value*
Specifies the peak burst size (PBS), that is, the most bytes per second allowed in a burst before all packets exceed the PIR. You must specify a value greater than 0. On ICX 6650 devices, the *pbs-value* is the rate in packets per second.

exceed-action
Specifies the action for traffic that is more than is configured in the *cir-value* variable. If you do not configure this keyword, traffic that exceeds the *cir-value* is dropped

drop
Specifies dropping traffic that exceeds the rate limit.

count
Enables counting the number of bytes and the conformance level per packet. The two-rate three-color marker (trTCM) mechanism described in RFC 2698 is used.

permit-at-low-pri
Specifies permitting packets that exceed the *cir-value* and forward them at the lowest priority.

remark-cos
Sets the 802.1p priority of dropped packets to 0, that is, it sets the COS/PCP field value to 0 for the low priority traffic for any packet exceeding the rate limit set by the traffic policy

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command deletes a traffic policy definition.

Traffic policies must be referenced by one or more ACLs before they can be effective. The policies are effective on ports to which the ACLs that reference them are bound.

NOTE
You cannot delete a traffic policy definition that a port is currently using. To delete a traffic policy, you must first unbind the associated ACL.

It is recommended that you specify a PBS value that is equal to or greater than the size of the largest possible IP packet in the stream.

Examples

This example configures a traffic policy named TPDA4 that specifies a CIR of 10000 Kbps, a CBS of 1600 Kbps, a PIR of 20000 Kbps, and a PBS of 1000 Kbps a and dropping any traffic that exceeds those limits.

```
device#configure terminal
device(config)#traffic-policy TPDA4 rate-limit adaptive cir 10000 cbs 1600 pir
20000 pbs 4000 exceed-action drop
```

traffic-policy rate-limit fixed

Configures an ACL-based fixed-rate traffic policy to define rate limits on packets. It either drops all traffic that exceeds the limit, or forwards it at the lowest priority level.

Syntax

traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **count**

traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action drop** [**count**]

traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

no traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **count**

no traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action drop** [**count**]

no traffic-policy *traffic-policy-def* **rate-limit fixed** *cir-value* **exceed-action permit-at-low-pri** [**count** | **remark-cos** [**count**]]

Command Default

No traffic policy is applied.

Parameters

traffic-policy-def

Specifies the name of the traffic policy definition, in no more than seven alphanumeric characters.

cir-value

Specifies the committed information rate (CIR) in Kbps, that is, the guaranteed rate of inbound traffic that is allowed on a port. The range is 64 through 1,000,000 Kbps. On ICX 6650 devices, the *cir-value* is the rate in packets per second. The range is 125 through 15,000,000 packets per second

count

Enables counting the number of bytes and the conformance level per packet. The single-rate three-color marker (srTCM) mechanism described in RFC 2697 is used.

exceed-action

Specifies the action for traffic that is more than is configured in the *cir-value* variable. If you do not configure this keyword, traffic that exceeds the *cir-value* is dropped

drop

Specifies dropping traffic that exceeds the rate limit.

count

Enables counting the number of bytes and the conformance level per packet. The single-rate three-color marker (srTCM) mechanism described in RFC 2697 is used.

permit-at-low-pri

Specifies permitting packets that exceed the *cir-value* and forward them at the lowest priority.

remark-cos

Sets the 802.1p priority of dropped packets to 0, that is, it sets the COS/PCP field value to 0 for the low priority traffic for any packet exceeding the rate limit set by the traffic policy

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command deletes a traffic policy definition.

Traffic policies must be referenced by one or more ACLs before they can be effective. The policies are effective on ports to which the ACLs that reference them are bound.

NOTE
You cannot delete a traffic policy definition that is currently in use on a port. To delete a traffic policy, you must first unbind the associated ACL.

Examples

This example configures a traffic policy named TPD1 that specifies a CIR of 100 Kbps and dropping any traffic that exceeds the limit.

```
device#configure terminal
device(config)#traffic-policy TPD1 rate-limit fixed 100 exceed-action drop
```

transmit-counter

Configures traffic counters that enable the device to count the packet types on a port or port region.

Syntax

transmit-counter *counter-ID* **port** *slot/port* { **only** | **region** } **vlan** { *vlan-id* | **all** } **prio** { *priority-queue* | **all** } **enable**

no transmit-counter *counter-ID* **port** *slot/port* { **only** | **region** } **vlan** { *vlan-id* | **all** } **prio** { *priority-queue* | **all** } **enable**

Command Default

Traffic counters are not configured.

Parameters

counter-ID
: Specifies the traffic counter. The range is from 1 to 64.

port *slot/port*
: Configures the port number on which to apply the enhanced traffic counters.

only
: Applies the enhanced traffic counters for the specified port only.

region
: Applies the enhanced traffic counters for all ports in the port region.

vlan *vlan-id*
: Configures the VLAN for which outbound traffic is counted. The value can range from 0 to 4095.

all
: Configures the outbound traffic to be counted for all the VLANs.

prio *priority-queue*
: Configures the traffic to be counted for the 802.1p priority queue. The range is from 0 to 7.

all
: Configures the traffic to be counted for all 802.1p priority queues.

Modes

Global configuration mode

Usage Guidelines

This feature is supported on FSX devices only.

You can configure traffic counters (also called transmit counters) that enable the Brocade device to count the broadcast, multicast, unicast, and dropped (dropped packets due to congestion and egress filtering) packet types on a port or port region.

This feature applies to physical ports only, including 10 Gbps Ethernet ports and LAG ports. It does not apply to virtual interfaces. For each port region, you can enable a maximum of two traffic counters, regardless of whether traffic counters are enabled on individual ports or on all ports in the port region.

Every time the enhanced traffic counters are read using the **show transmit-counter values** command, the counters are cleared (reset to zero).

The **no** form of the command removes the traffic counters.

Examples

The following example shows how to configure traffic counters for outbound traffic in a specific port region.

```
device(config)# transmit-counter 1 port 1/1 region vlan all prio all enable
```

The following example shows how to configure traffic counters for outbound traffic on a specific port.

```
device(config)#transmit-counter 4 port 1/18 only vlan 1 prio 7 enable
```

trunk-threshold

Configures the threshold value for the number of active member ports in a LAG, below which all the ports in a LAG group are disabled.

Syntax

trunk-threshold *number*

no trunk-threshold *number*

Command Default

The t runk threshold is set to 1.

Parameters

number

Specifies the number of ports as the threshold number. You can specify a threshold from 1 (the default) up to the number of ports in the LAG group.

Modes

LAG configuration mode

Usage Guidelines

When a LAG is shut down because the number of ports drops below the configured threshold, the LAG is kept intact and it is re-enabled if enough ports become active to reach the threshold.

NOTE
The **trunk-threshold** command cannot be used in conjunction with protected link groups.

NOTE
The **trunk-threshold** command is only applicable for the configuration of static LAGs.

The **trunk-threshold** command should be configured only at one end of the LAG. If it is set on both ends, link failures will result in race conditions and the LAG not function properly. Use a short LACP timeout when setting the **trunk-threshold** value equal to the number of links in the LAG or connecting to third-party devices.

The **no** form of the command removes the **trunk-threshold** configuration.

Examples

The following example shows how to establish a LAG group consisting of four ports, and then establish a threshold for this LAG group of three ports. If the number of active ports drops below three, then all the ports in the LAG group are disabled.

```
device(config)# lag blue static
device(config-lag-blue)# ports ethernet 1/3/1 to 1/3/4
device(config-lag-blue)# trunk-threshold 3
```

trust dscp

Configures the devices to honor DSCP-based QoS for routed and switched traffic.

Syntax

trust dscp

no trust dscp

Command Default

The interface honors the Layer 2 CoS value.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables the devices to honor DSCP-based QoS.

NOTE
The **trust dscp** command is not supported with 802.1p priority override.

Examples

the following example shows how to honor DSCP-based QoS.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# trust dscp
```

trust-port

Configures ports of a Web Authentication VLAN as trusted ports.

Syntax

trust-port ethernet *stack/slot/port* [**to** *stack/slot/port*]

no trust-port ethernet *stack/slot/port* [**to** *stack/slot/port*]

Command Default

Ports of a Web Authentication VLAN are not trusted.

Parameters

ethernet *stack/slot/port*

Configures the specified Ethernet interface as a trusted port.

to *stack/slot/port*

Configures a range of Ethernet interfaces as trusted.

Modes

Web Authentication configuration mode

Usage Guidelines

All hosts connected to the trusted ports need not authenticate and are automatically allowed access to the network.

The **no** form of the command removes the trusted port configuration.

Examples

The following example shows how to configure an Ethernet interface as a trusted port.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# trust-port ethernet 1/1/1
```

The following example shows how to configure a range of ports as trusted.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# trust-port ethernet 1/1/1 to 1/1/10
```

tunnel destination

Configures the destination address for a specific tunnel interface.

Syntax

tunnel destination { *ip address* }

no tunnel destination { *ip address* }

Command Default

No tunnel interface destination is configured.

Parameters

ip address

Specifies the IPv4 address of an interface.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no tunnel destination** command to remove the configured destination for the tunnel interface.

You must ensure that a route to the tunnel destination exists on the tunnel source device and create a static route if necessary.

Examples

This example configures the IP address 10.1.2.3 as the destination address for a specific tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 3
device(config-tnif-3)# tunnel destination 10.1.2.3
```

Related Commands

tunnel source

tunnel mode gre ip

Enables generic routing encapsulation (GRE) over on a tunnel interface and specifies that the tunneling protocol is IPv4.

Syntax

tunnel mode gre ip

no tunnel mode gre ip

Command Default

GRE is disabled.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no tunnel mode gre ip** command to disable the GRE IP tunnel encapsulation method for the tunnel interface.

Examples

This example enables GRE IP encapsulation on a tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 3
device(config-tnif-3)# tunnel mode gre ip
```

Related Commands

interface tunnel

tunnel mode ipv6ip

Configures the tunnel mode as a manual IPv6 tunnel.

Syntax

tunnel mode ipv6ip

no tunnel mode ipv6ip

Command Default

Tunnel is not configured.

Modes

Interface tunnel configuration mode

Usage Guidelines

You can use a manually configured tunnel to connect two isolated IPv6 domains. You should deploy this point-to-point tunneling mechanism if you need a permanent and stable connection.

The **no** form of the command removes the manually configured tunnel.

Examples

The following example sets the tunnel mode as a manual IPv6 tunnel.

```
device(config)# interface tunnel 1
device(config-tnif-1)# tunnel source ethernet 1/1/1
device(config-tnif-1)# tunnel destination 10.162.100.1
device(config-tnif-1)# tunnel mode ipv6ip
device(config-tnif-1)# ipv6 enable
```

tunnel source

Configures the source address or a source interface for a specific tunnel interface.

Syntax

tunnel destination { *ip address* | **ethernet** *stackid / slot / port* | **loopback** *number* | **ve** *vlan_id*}

no tunnel destination { *ip address* | **ethernet** *stackid / slot / port* | **loopback** *number* | **ve** *vlan_id*}

Command Default

No source address or interface is configured.

Parameters

ip address
Specifies the IPv4 address of an interface.

ethernet *stackid / slot / port*
Specifies an Ethernet interface.

loopback *number*
Specifies an loopback port.

ve *vlan_id*
Specifies a VE interface.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no tunnel source** command to remove the configured source for the tunnel interface.

The tunnel source address should be one of the router IP addresses configured on a physical, loopback, or VE interface, through which the other end of the tunnel is reachable. The source interface must have at least one IP address configured on it.

Examples

This example configures the IP address 10.1.2.4 as the source address for a specific tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 3
device(config-tnif-3)# tunnel source 10.1.2.4
```

This example sets an Ethernet interface as a source tunnel.

```
device# configure terminal
device(config)# interface tunnel 1
device(config-tnif-1)# tunnel source ethernet 3/1
```

Related Commands

tunnel destination

unknown-unicast limit

Enables rate limiting on a port, enables Syslog logging of unknown-unicast packets, or sets a packet drop threshold value.

Syntax

unknown-unicast limit *num* **kbps** [**log** | **threshold** *packet_threshold* **action port-shutdown** [*shutdown_seconds*]]

no unknown-unicast limit *num* **kbps** [**log** | **threshold** *packet_threshold* **action port-shutdown** [*shiudown_seconds*]]

Command Default

Unknown unicast rate limiting, logging, and port dampening are disabled.

Parameters

num

Specifies the maximum number of broadcast packets per second ranging from 1 to 8388607; or when followed by **kbps**, *num* is the number of kilo bits per second (kbps) permitted for byte-based limiting. The value in this case is 1 to the maximum port speed. Use 0 to disable rate limiting.

kbps

Enables byte-based limiting. The value can be 1 to Max Port Speed.

log

Enables Syslog logging when the unknown-unicast limit exceeds *num* **kpbs** .

threshold

The packet drop count threshold.

packet_threshold

Specifies the number of packets (in kilo bytes) that when exceeded, the port is shutdown. The value ranges from 1 KB to 10 GB.

action

The action to be taken.

port-shutdown

Set the **action** as a port shutdown event.

shutdown_seconds

The amount of time, in seconds, the port is shutdown. The default is 300 seconds and the range is from 1 to 65535 seconds.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to disable rate limiting on a port, Syslog logging of excess packets, or the packet drop threshold value.

If the port *shutdown_seconds* parameter is set to 0, the port is kept in ERR-DISABLE state until you re-enabled it.

Examples

The following example enables a unknown-unicast rate limit of 131072 kbps.

```
device(config)# interface ethernet 9/1/1
device(config-if-e1000-9/1/1)# unknown-unicast limit 131072 kbps
```

The following example enables unknown-unicast limit logging when the configured unknown-unicast limit exceeds 100 Kbps.

```
device(config)# interface ethernet 1/2/1
device(config-if-e10000-1/2/1)# unknown-unicast limit 100 kbps log
```

The following example shuts down the port for 300 seconds (default) when the packet drop threshold value exceeds 1000 KBs.

```
device(config)# interface ethernet 1/2/1
device(config-if-e10000-1/2/1)# unknown-unicast limit 100 kbps threshold 1000 action port-shutdown
```

History

Release version	Command history
8.0.10	The command was introduced.
8.0.30h	The command was modified to include the keyword **threshold**.
8.0.40a	The command was modified to include the keyword **log**.

unmount disk0

Unmounts the external USB.

Syntax

unmount disk0

Modes

User EXEC mode.

Examples

The following example unmounts the external USB.

```
device# unmount disk0
```

History

Release version	Command history
08.0.30	This command was introduced.

untagged

Adds untagged ports to the VLAN.

Syntax

untagged ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no untagged ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Parameters

ethernet *stackid/slot/port*

Configures and adds the ports as untagged.

to *stackid/slot/port*

Configures and adds a range of ports to be added as untagged ports.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command removes the untagged ports on the VLAN.

Examples

The following example shows how to add untagged ports to a port-based VLAN.

```
device(config)# vlan 222 by port
device(config-vlan-222)# untagged ethernet 1/1/1 to 1/1/8
```

update-lag-name

Changes the name of an existing LAG without causing any impact on the functionality of the LAG.

Syntax

update-lag-name *new-name*

Parameters

new-name

Specifies the new name for the LAG.

Modes

LAG configuration mode

Usage Guidelines

The new name must be unique and unused.

Examples

The following example renames LAG blue to blue1.

```
device(config)# lag blue static
device(config-lag-blue)# update-lag-name blue1
INFORMATION: Lag blue with ID 1 is updated to new name blue1
device(config)#
```

History

Release version	Command history
08.0.30	This command was introduced.

update-time (BGP)

Configures the interval at which BGP next-hop tables are modified. BGP next-hop tables should always have IGP (non-BGP) routes.

Syntax

update-time *sec*

no update-time *sec*

Command Default

This option is disabled.

Parameters

sec

Update time in seconds. Range is from 0 through 30. Default is 5 seconds.

Modes

BGP configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

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

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.

The update time determines how often the device computes the routes (next-hops). Lowering the value set by the **update-time** command increases the convergence rate.

By default, the device updates the BGP next-hop tables and affected BGP routes five seconds following IGP route changes. Setting the update time value to 0 permits fast BGP convergence for situations such as a link failure or IGP route changes, starting the BGP route calculation in sub-second time.

NOTE
Use the **advertisement-interval** command to determine how often to advertise IGP routes to the BGP neighbor.

Examples

This example permits fast convergence.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# update-time 0
```

This BGP4+ example sets the update time interval to 30.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# update-time 30
```

uplink-switch

Defines uplink ports and enables uplink switching.

Syntax

uplink-switch ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

no uplink-switch ethernet *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*] ...]

Command Default

Uplink ports are not configured.

Parameters

ethernet *stackid/slot/port*

Defines the Ethernet ports as an uplink port and enables uplink switching on the ports.

to *stackid/slot/port*

Defines a range of ports as uplink ports and enables uplink switching on these ports.

Modes

VLAN configuration mode

Usage Guidelines

Uplink switching is supported on MCT VLANs. ICLs and CCEPs can be configured as uplink switch ports. Both cluster devices should have exactly the same uplink switch port memberships with respect to the ICL and CCEPs.

NOTE

Do not use this command when protocol VLANs or PVLANs are in the same VLAN.

The **no** form of the command disables uplink switching on ports.

Examples

The following example configures uplink ports within a port-based VLAN.

```
device(config)# vlan 10 by port
device(config-vlan-10)# untagged ethernet 1/1/1 to 1/1/24
device(config-vlan-10)# untagged ethernet 1/2/1 to 1/2/2
device(config-vlan-10)# uplink-switch ethernet 1/2/1 to 1/2/2
```

use-radius-server

Maps a RADIUS server to a port.

Syntax

use-radius-server *ip-address*

no use-radius-server *ip-address*

Command Default

The RADIUS server is not mapped to any port.

Parameters

ip-address

The IP address of the RADIUS server.

Modes

Interface configuration mode

Usage Guidelines

Once the RADIUS server is mapped to a port, the port sends the RADIUS request to the configured RADIUS server.

The **no** form of the command removes the mapping of the RADIUS server to the port.

Examples

The following example shows how to map a RADIUS server to the interface 1/1/3 (port 3). Port 3 sends a RADIUS request to 10.10.10.103 first, because it is the first server mapped to the port. If the request fails, the server will go to 10.10.10.110.

```
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# use-radius-server 10.10.10.103
device(config-if-e1000-1/1/1)# use-radius-server 10.10.10.110
```

username

Creates or updates user account.

Syntax

username *username-string* { **access-time** *begin-time* [**to** *end-time*] | **enable** | **expires** *days* | [**privilege** *privilege-level*] { **password** *password-string* | **create-password** *password-string* | **nopassword** } }

no username *username-string* { **access-time** *begin-time* [**to** *end-time*] | **enable** | **expires** *days* | [**privilege** *privilege-level*] { **password** *password-string* | **create-password** *password-string* | **nopassword** } }

Command Default

The user account is not created.

Parameters

username-string

The configured username. You can enter up to 48 characters.

access-time *begin-time* **to** *end-time*

Configures the beginning access time and ending access time for the user.

enable

Enables the user for login access after the login access is disabled.

expires *days*

Configures the password expiration time in days. The valid values are from 1 through 365.

privilege *privilege-level*

Sets the user's privilege level. You can specify one of the following levels:

0

Super User level (full read-write access). The default privilege level is 0.

4

Port Configuration level

5

Read Only level

password *password-string*

Configures the password for the user. You can enter up to 48 characters.

create-password *password-string*

Creates an encrypted password for the user. You can enter up to 48 characters.

nopassword

Configures the user to log in without a password.

Modes

Global configuration mode

Usage Guidelines

If the **strict password enforcement** command is enabled on the device, for the password string, you must enter a minimum of eight characters containing the following combinations:

- At least two uppercase characters
- At least two lowercase characters
- At least two numeric characters
- At least two special characters

NOTE
You must be logged in with Super User access (privilege level 0) to add user accounts or configure other access parameters.

You can use the **show user** command to display the user account details.

The **no** form of the command removes the user or the user updates.

Examples

The following example shows how to configure the access time for a user.

```
device(config)# username user1 access-time 00:00:00 to 12:00:00
```

The following example shows how to enable a user account if it is disabled.

```
device(config)# username user1 enable
```

The following example shows how to set the user password to expire.

```
device(config)# username user expires 30
```

The following example shows how to configure the privilege level of Super User access (0) for a user.

```
device(config)# username user1 privilege 0 password *******
```

The following example shows how to create a user account without a password.

```
device(config)# username user1 nopassword
```

username (Local database)

Creates a user record in the local user database.

Syntax

username *username* **password** *password-string*

no username *username* [**password** *password-string*]

Command Default

User records are not created.

Parameters

username

Specifies the username for the user as an ASCII string. You can specify up to 31 characters.

password *password-string*

Specifies the password for the user. You can specify up to 29 characters.

Modes

Local user database configuration mode

Usage Guidelines

You can add up to 30 usernames and passwords to a local user database.

The **no** form of the command removes the user record from the local user database.

Examples

The following example creates a new user account and adds it to a local user database.

```
device(config)# local-userdb userdb1
device(config-localuserdb-userdb1)# username XYZ password A5!fk3p
```

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 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 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 in IPv4 and IPv6 VRRPv3 instances.

```
IPv6 :
Brocade(config)# interface ve 3
Brocade(config-vif-3)# ipv6 vrrp vrid 2
Brocade(config-vif-3-vrid-2)# use-v2-checksum

IPv4 :
Brocade(config)# interface ve 3
Brocade(config-vif-3)# ipv4 vrrp vrid 2
Brocade(config-vif-3-vrid-2)# version v3
Brocade(config-vif-3-vrid-2)# use-v2-checksum
```

History

Release version	Command history
08.0.01	This command was introduced for IPv6 VRRPv3 sessions running on FastIron device images.
08.0.10b	This command was modified for IPv4 VRRPv3 sessions running on FastIron device images.

use-vrrp-path (RIP)

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 enabled.

Modes

RIP configuration mode

Usage Guidelines

The command applies only to devices configured for Virtual Router Redundancy Protocol (VRRP) or for VRRP Extended (VRRPE). The same command syntax is used for both protocols. The command applies only if you have specified an IP address to back up and is valid only on Layer 3 Switches.

Normally for Layer 3, a VSRP backup includes route information in RIP advertisements for an interface with a VRRP or VRRP-E backup. As a result, other Layer 3 switches receive multiple paths for the backed-up interface and may sometimes unsuccessfully use the path to the backup router rather than the path to the master.

Use the command to suppress RIP advertisements from the backup router on the interface. This ensures that the interface advertises paths to the master router only.

The **no** form of this command resets the default behavior, and the interface sends RIP advertisements from the backup router.

Examples

The following example shows how to suppress RIP advertisements from backup VRRP or VRRP-E routers.

```
device(config)# router rip
device(config-rip-router)# use-vrrp-path
```

vendor-class

Specifies the vendor type (option 60) and configuration value for a DHCP client.

Syntax

vendor-class { **ascii** } *ascii string*

Parameters

ascii

Specifies the ascii keyword.

ascii string

Specifies the ASCII string value of the DHCP client.

Modes

DHCP server pool configuration mode

Examples

The following example specifies option 60 using the ASCII option for a Ruckus AP.

```
device# configure terminal
device(config)# ip dhcp-server-pool ruckus
device(ip dhcp-server pool ruckus)#    vendor-class ascii "Ruckus CPE"
device(ip dhcp-server pool ruckus)# deploy
```

History

Release version	Command history
08.0.30mb	An additional example was added in the Examples section for option 60.

verify

Allows to verify boot images based on hash codes, and to generate hash codes where needed.

Syntax

verify { **md5** | **sha1** | **crc32** } { **primary** | **secondary** } [*string*]

Parameters

md5
: Verifies the file content using MD5 checksum and generates a 16-byte hash code.

sha1
: Verifies the file content using SHA and generates a 20-byte hash code

cec32
: Verifies the file content using CEC32 and generates a 4-byte hash code

primary
: Verifies the primary boot image.

secondary
: Verifies the secondary boot image.

string
: A valid image filename name or a generated hash code value.

Modes

Privileged EXEC mode

Usage Guidelines

This feature lets you select from three data integrity verification algorithms:

- MD5 - Message Digest algorithm (RFC 1321)
- SHA1 - US Secure Hash Algorithm (RFC 3174)
- CRC - Cyclic Redundancy Checksum algorithm

Examples

The following example shows how the **verify** command can be used to generate an MD5 hash value for the secondary image.

```
device# verify md5 secondary
device#.........................Done
Size = 2044830, MD5 01c410d6d153189a4a5d36c955653862
```

The following example shows how the **verify** command can be used to generate a SHA-1 hash value for the secondary image.

```
device# verify sha secondary
device#.........................Done
Size = 2044830, SHA1 49d12d26552072337f7f5fcaef4cf4b742a9f525
```

The following example shows how the **verify** command can be used to generate a CRC32 hash value for the secondary image.

```
device# verify crc32 secondary
device#.....................Done
Size = 2044830, CRC32 b31fcbc0
```

The following example shows how the **verify** command can be used to verify the hash value of a secondary image with a known value.

```
device# verify md5 secondary 01c410d6d153189a4a5d36c955653861
device#.....................Done
Size = 2044830, MD5 01c410d6d153189a4a5d36c955653861
Verification SUCEEDED.
```

The following example shows how the **verify** command can be used to verify the SHA-1 hash value of a secondary image with a known value.

```
device# verify sha secondary 49d12d26552072337f7f5fcaef4cf4b742a9f525
device#.....................Done
Size = 2044830, sha 49d12d26552072337f7f5fcaef4cf4b742a9f525
Verification SUCCEEDED.
```

The following example shows how the **verify** command can be used to verify the CRC32 hash value of a secondary image with a known value.

```
device# verify crc32 secondary b31fcbc0
device#.....................Done
Size = 2044830, CRC32 b31fcbc0
Verification SUCCEEDED
```

version

Allows you to select either version 2 or version 3 of VRRP.

Syntax

version {**v2** | **v3**}

no version v3

Command Default

The default is VRRP version 2.

Parameters

v2	Selects version 2 of VRRP.
v3	Selects version 3 of VRRP.

Modes

VRRP virtual router ID configuration.

Usage Guidelines

You can choose either version 2 or version 3 of IPv4 VRRP. The default IPv4 VRRP configuration is VRRPv2. The VRRPv3 functionality is enabled only after you configure version 3. Use the **no version v3** or **version v2** commands to roll back to the default (VRRPv2).

Examples

The following example configures the VRRP owner router for IPv4.

```
device(config)#router vrrp
device(config)#interface ethernet 1/6
device(config-if-1/6)#ip-address 192.53.5.1
device(config-if-1/6)#ip vrrp vrid 1
device(config-if-1/6-vrid-1)#owner
device(config-if-1/6-vrid-1)# version v3 | v2
device(config-if-1/6-vrid-1)#ip-address 192.53.5.1
device(config-if-1/6-vrid-1)#activate
```

The following example configures the VRRP backup router for IPv4.

```
device(config)#router vrrp
device(config)#interface ethernet 1/5
device(config-if-1/5)#ip-address 192.53.5.3
device(config-if-1/5)#ip vrrp vrid 1
device(config-if-1/5-vrid-1)#backup
device(config-if-1/6-vrid-1)# version v3 |v2
device(config-if-1/5-vrid-1)#advertise backup
device(config-if-1/5-vrid-1)#ip-address 192.53.5.1
device(config-if-1/5-vrid-1)#activate
```

History

Release version	Command history
08.0.10	This command was introduced.

violation

Configures the device to take actions when a security violation occurs; either drop packets from the violating address (and allow packets from secure addresses), or disable the port for a specified time.

Syntax

violation { **restrict** *age* | **shutdown** *time* }

no violation { **restrict** *age* | **shutdown** *time* }

Command Default

The action to be taken when security violation occurs is not configured.

Parameters

restrict

Configures the device to drop packets from a violating address and allow packets from secure addresses.

age

Configures the time, in minutes, for which the device drops packets from a violating address. The valid values are from 0 through 1440 minutes. The default is 5 minutes. Specifying 0 drops packets from the violating address permanently.

shutdown *time*

Configures the device to disable the port for a specified amount of time, in minutes, when a security violation occurs. The valid values are from 0 through 1440 minutes. Specifying 0 shuts down the port permanently when a security violation occurs.

Modes

Port security configuration mode

Port security interface configuration mode

Usage Guidelines

A security violation can occur when a user tries to connect to a port where a MAC address is already locked, or the maximum number of secure MAC addresses has been exceeded. When a security violation occurs, an SNMP trap and syslog message are generated. You can configure the device to take one of two actions when a security violation occurs; either drop packets from the violating address (and allow packets from secure addresses), or disable the port for a specified time.

When the **restrict** option is used, the maximum number of MAC addresses that can be restricted is 128. If the number of violating MAC addresses exceeds this number, the port is shut down. An SNMP trap and the following syslog message are generated: "Port Security violation restrict limit 128 exceeded on interface ethernet port_id ". This is followed by a port shutdown syslog message and trap. Aging for restricted MAC addresses is done in software. There can be a worst case inaccuracy of one minute from the specified time. The restricted MAC addresses are denied in hardware.

The **no** form of the command removes the security violation action settings.

Examples

The following example configures the device to drop packets from a violating address and allow packets from secure addresses.

```
device(config)# interface ethernet 1/7/11
device(config-if-e1000-1/7/11)# port security
device(config-port-security-e1000-1/7/11)# violation restrict
```

The following example shows how to specify the number of minutes that the device drops packets from a violating address.

```
device(config)# interface ethernet 1/7/11
device(config-if-e1000-1/7/11)# port security
device(config-port-security-e1000-1/7/11)# violation restrict 5
```

The following example shuts downs the port for 5 minutes when a security violation occurs.

```
device(config)# interface ethernet 1/7/11
device(config-if-e1000-1/7/11)# port security
device(config-port-security-e1000-1/7/11)# violation shutdown 5
```

virtual-ip

Configures the IP address of the external captive portal server as the virtual IP address.

Syntax

virtual-ip { *ip-address* | *ASCII string* }

no virtual-ip { *ip-address* | *ASCII string* }

Command Default

A virtual IP address is not configured.

Parameters

ip-address

Specifies the IP address of the external captive portal server where the web pages are hosted.

ASCII string

Specifies the server name of the external captive portal server where the web pages are hosted.

Modes

Captive portal configuration mode

Usage Guidelines

The **no** form of the command removes the virtual IP address configuration.

Examples

The following example configures the IP address of the external captive portal server as the virtual IP address.

```
device(config)# captive-portal cp_brocade
device(config-cp-cp_brocade)# virtual-ip 10.21.240.42
```

History

Release version	Command history
8.0.40	This command was introduced.
8.0.30j	This command was added to FastIron 8.0.30j

virtual-port

Configures the HTTP port number to facilitate HTTP services for the clients in external Web Authentication.

Syntax

virtual-port *http-port-number*

no virtual-port *http-port-number*

Command Default

A virtual port number is not configured.

Parameters

http-port-number

Specifies the port number. By default, HTTPS is used and the default port number for HTTPS is 443.

Modes

Captive portal configuration mode

Usage Guidelines

The protocol configured in the Captive Portal profile must be the same as the protocol configured as part of web management access using the **web-management** command.

You can also specify HTTP mode and the default port number for HTTP is 80.

The **no** form of the command removes the virtual port number configuration.

Examples

The following example configures the virtual port number used by HTTP.

```
device(config)# captive-portal cp_brocade
device(config-cp-cp_brocade)# virtual-port 80
```

History

Release version	Command history
8.0.40	This command was introduced.
8.0.30j	This command was added to FastIron 8.0.30j

vlan

Creates VLANs.

Syntax

vlan *vlan-id* [**to** *vlan-id* | [*vlan-id* **to** *vlan-id* | *vlan-id*] ...] [**name** *string*] [**by port**]

no vlan *vlan-id* [**to** *vlan-id* | [*vlan-id* **to** *vlan-id* | *vlan-id*] ...] [**name** *string*] [**by port**]

Command Default

The default VLAN is 1.

Parameters

vlan-id

Specifies the VLAN ID.

to *vlan-id*

Creates a range of VLANs.

name *string*

Specifies the name of the VLAN. The name can be up to 32 characters in length.

by port

Configures the VLAN as a port-based VLAN.

Modes

Global configuration mode

Usage Guidelines

You can configure up to 1023 port-based VLANs on a device (4063 on the Brocade ICX 6650) running Layer 2 code or 4061 port-based VLANs on a device running Layer 3 code. Each port-based VLAN can contain either tagged or untagged ports. A port cannot be a member of more than one port-based VLAN unless the port is tagged.

NOTE
VLAN IDs 4087, 4090, and 4093 are reserved for Brocade internal use only. VLAN 4094 is reserved for use by Single STP. Also, VLAN IDs 4091 and 4092 may be reserved for Brocade internal use only. If you want to use VLANs 4091 and 4092 as configurable VLANs, you can assign them to different VLAN IDs

The **no** form of the command removes the VLAN.

Examples

The following example shows how to create a port-based VLAN.

```
device(config)# vlan 222 by port
```

The following example shows the port-based VLAN configuration.

```
device(config)# vlan 10 name IP_VLAN by port
device(config-vlan-10)# untagged ethernet 1/1/1 to 1/1/6
added untagged port ethe 1/1/1 to 1/1/6 to port-vlan 10.
```

The following example shows how to create continuous and discontinuous VLANs.

```
device(config)# vlan 2 to 7 20 25
device(config-mvlan-2*25)#
```

The following example shows how to create continuous VLANs.

```
device(config)# vlan 2 to 7
device(config-mvlan-2-7)#
```

The following example shows how to create discontinuous VLANs.

```
device(config)# vlan 2 4 7
device(config-mvlan-2*7)#
```

vlan-group

Configures a VLAN group.

Syntax

vlan-group *num* **vlan** *vlan-id* [**to** *vlan-id*]

no vlan-group *num* **vlan** *vlan-id* [**to** *vlan-id*]

Command Default

A VLAN group is not configured.

Parameters

num

Specifies the group VLAN ID. The values can be from 1 through 32.

vlan *vlan-id*

Specifies the starting VLAN ID to create a VLAN group.

to *vlan-id*

Specifies the ending VLAN ID. This is a continuos range of individual VLAN IDs.

Modes

Global configuration mode

Usage Guidelines

Specify the low VLAN ID first and the high VLAN ID second. The command adds all of the specified VLANs to the VLAN group. You can add up to 256 VLANs with the command at one time.

If a VLAN within the range you specify is already configured, or if the range contains more than 256 VLANs, the VLAN group is not created and an error message is displayed.

To add more than 256 VLANs, enter the **add-vlan** command in VLAN group configuration mode.

The **no** form of the command deletes the VLAN group.

Examples

The following example shows the VLAN group configuration.

```
device(config)# vlan-group 1 vlan 2 to 255
```

voice-vlan

Creates a voice VLAN ID for a port, or for a group of ports on which a voice over IP (VOIP) phone is connected.

Syntax

voice-vlan *voice-vlan-num*

no voice-vlan *voice-vlan-num*

Command Default

Voice VLAN ID is not configured.

Parameters

voice-vlan-num

Specifies a valid VLAN ID. The valid values are between 1 and 4095.

Modes

Interface configuration mode

Usage Guidelines

When you configure a voice VLAN ID on the port to which the VoIP phone is connected the device automatically detects and reconfigures a VoIP phone when it is physically moved from one port to another within the same device.

When the Brocade device receives the VoIP phone query, it sends the voice VLAN ID in a reply packet back to the VoIP phone. The VoIP phone then configures itself within the voice VLAN.

As long as the port to which the VoIP phone is connected has a voice VLAN ID, the phone will configure itself into that voice VLAN. If you change the voice VLAN ID, the software will immediately send the new ID to the VoIP phone, and the VoIP phone will reconfigure itself with the new voice VLAN.

Some VoIP phones may require a reboot after configuring or reconfiguring a voice VLAN ID.

The **no** form of the command removes the voice VLAN ID from the port.

Examples

The following example shows how to create VLAN ID for a port.

```
device(config)# interface ethernet 2/1/1
device(config-if-e1000-2/1/1)# voice-vlan 1001
```

The following example shows how to create VLAN ID for a group of ports.

```
device(config)# interface ethernet 1/1/2 to 1/1/10
device(config-if-e1000-1/1/2-1/1/10)# voice-vlan 1005
```

vrf

Configures a Virtual Routing and Forwarding (VRF) and enters VRF configuration mode.

Syntax

vrf *vrf-name*

no vrf *vrf-name*

Command Default

VRF is not created.

Parameters

vrf-name

Specifies the name of the VRF. The name can be upto 255 characters.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the VRF.

Examples

The following example shows how to configure a VRF and enter into the VRF configuration mode.

```
device(config)# vrf vrf1
device(config-vrf-vrf1)#
```

vsrp

Configures VSRP on a device.

Syntax

vsrp vrid *vrid-num*

no vsrp vrid *vrid-num*

vsrp auth-type { **no-auth** | **simple-text-auth** *password* }

no vsrp auth-type { **no-auth** | **simple-text-auth** *password*}

Command Default

VSRP is not configured.

Parameters

vrid *vrid-num*
Configures the VRID for the VLAN. The VRID range is from 1 through 255.

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.

If the interfaces use simple password authentication, the VRID configured on the interfaces must use the same authentication type and the same password.

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
```

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-aware

Configures the security features on a VSRP-aware device.

Syntax

vsrp-aware vrid *vrid* **tc-vlan-flush**

no vsrp-aware vrid *vrid* **tc-vlan-flush**

vsrp-aware vrid *vrid* { **no-auth** | **simple-text-auth** *password* } [**port-list ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]]

no vsrp-aware vrid *vrid* { **no-auth** | **simple-text-auth** *password* } [**port-list ethernet** *stackid/slot/port* [**to** *stackid/slot/port* | [**ethernet** *stackid/slot/port* **to** *stackid/slot/port* | **ethernet** *stackid/slot/port*]...]]

Command Default

VSRP-aware security features are not configured.

Parameters

vrid *vrid*
Specifies the VRID of the VSRP device. The valid range is from 1 through 255.

tc-vlan-flush
Flushes the MAC addresses learned on the VSRP-aware VLAN upon topology change.

no-auth
Configures no authentication as the preferred VSRP-aware security method. The VSRP device will not accept incoming packets that have authentication strings.

simple-text-auth *password*
Defines an authentication string to accept incoming VSRP Hello packets. The password can be up to 8 characters in length.

port-list
Configures the range of ports to include in the configuration.

ethernet *stackid/slot/port*
Specifies the Ethernet interface.

to *stackid/slot/port*
Specifies the range of Ethernet interfaces.

Modes

VLAN configuration mode

Usage Guidelines

When the **tc-vlan-flush** option is enabled, MAC addresses will be flushed at the VLAN level, instead of at the port level. MAC addresses will be flushed for every topology change received on the VSRP-aware ports. When you configure the **tc-vlan-flush** option on a VSRP-aware device, and the device receives VSRP Hello packets from the VSRP master, VSRP authentication is automatically configured. However, if the VSRP-aware device does not receive VSRP Hello packets from the VSRP master when the **tc-vlan-flush** option is configured, you must manually configure VSRP authentication.

The **no** form of the command clears the security features on the VSRP-aware device.

Examples

The following example shows how to configure the MAC addresses to be flushed at the VLAN level.

```
device(config)# vlan 200
device(config-vlan-200)# vsrp-aware vrid 11 tc-vlan-flush
```

The following example shows how to configure a simple authentication string for the VSRP.

```
device(config)# vlan 10
device(config-vlan-10)# vsrp-aware vrid 3 simple-text-auth pri-key
```

The following example shows how to configure no authentication for the VSRP.

```
device(config)# vlan 10
device(config-vlan-10)# vsrp-aware vrid 2 no-auth
```

The following example shows how to configure no authentication for a range of Ethernet ports.

```
device(config)# vlan 10
device(config-vlan-10)# vsrp-aware vrid 4 no-auth port-list ethernet 1/1/1 to 1/1/4
```

web access-group

Configures an ACL that restricts web management access to the device.

Syntax

web access-group { *acl-num* | *acl-name* | **ipv6** *ipv6-acl-name* }

no web access-group { *acl-num* | *acl-name* | **ipv6** *ipv6-acl-name* }

Command Default

Web management access is not restricted.

Parameters

acl-num
: The standard access list number. The valid values are 1 through 99.

acl-name
: The standard access list name.

ipv6 *ipv6-acl-name*
: The IPv6 access list name.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the restriction of web management access for an ACL.

Examples

The following example shows how to configure an ACL that restricts web management access to the device. In this example, ACL 12 is configured. The device denies web management access from the IP addresses listed in ACL 12 and permits web management access from all other IP addresses. Without the last ACL entry for permitting all packets, this ACL would deny web management access from all IP addresses.

```
device(config)# access-list 12 deny host 209.157.22.98 log
device(config)# access-list 12 deny 209.157.23.0 0.0.0.255 log
device(config)# access-list 12 deny 209.157.24.0/24 log
device(config)# access-list 12 permit any
device(config)# web access-group 12
device(config)# write memory
```

web client

Restricts web management access to a host with a specified IP address.

Syntax

web client {*ip-address* | **ipv6** *ipv6-address* }

no web client {*ip-address* | **ipv6** *ipv6-address* }

Command Default

Web management access is not restricted.

Parameters

ip-address

The IPv4 address of the host to which the web management access is restricted.

ipv6 *ipv6-address*

The IPv6 address of the host to which the web management access is restricted.

Modes

Global configuration mode

Usage Guidelines

You can specify only one IP address with one command. However, you can enter the command ten times to specify up to ten IP addresses.

The **no** form of the command removes the web management access restriction.

Examples

The following example shows how to restrict web management access to the host with IP address 192.168.10.1.

```
device(config)# web client 192.168.10.1
```

webauth

Configures a Web Authentication VLAN and enters the Web Authentication configuration mode.

Syntax

webauth

no webauth

Modes

VLAN configuration mode

Usage Guidelines

Use the **enable** command in the Web Authentication configuration mode to enable Web Authentication.

Tthe **no** form of the command removes the Web Authentication VLAN.

Examples

The following example shows how to configure a Web Authentication VLAN.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config(config-vlan-10-webauth)#
```

The following example deletes a Web Authentication VLAN.

```
device(config)# vlan 10
device(config-vlan-10)# no webauth
```

webauth-redirect-address

Configures a redirect address for Web Authentication to prevent the display of error messages saying that the certificate does not match the name of the site.

Syntax

webauth-redirect-address *address-string*

no webauth-redirect-address [*address-string*]

Command Default

By default, the Web Authentication address returned to the browser is the IP address of the switch.

Parameters

address-string

Specifies the redirect address. You can specify up to 64 alphanumeric characters.

Modes

Global configuration mode

Web Authentication configuration mode

Usage Guidelines

You can enter any value for the address string , but entering the name on the security certificate prevents the display of error messages saying that the security certificate does not match the name of the site.

On a Layer 2 device, the command is supported in Global configuration mode and on a Layer 3 device the command is supported in Web Authentication configuration mode.

The **no** form of the command resets the redirect address to that of the IP address of the switch.

Examples

The following example shows how to set the Web Authentication redirect address on a Layer 3 switch.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webauth-redirect-address my.domain.net
```

web-management

Configures web management access options.

Syntax

web-management [**enable** { **vlan** *vlan-id* | **ethernet** *stack/slot/port* [**to** *stack/port/slot* | [**ethernet** *stack/slot/port* **to** *stack/port/slot* | **ethernet** *stack/slot/port*]...] }]

no web-management [**enable** { **vlan** *vlan-id* | **ethernet** *stack/slot/port* [**to** *stack/port/slot* | [**ethernet** *stack/slot/port* **to** *stack/port/slot* | **ethernet** *stack/slot/port*]...] }]

web-management [**allow-no-password** | **connection-receive-timeout** *timeout-value* | **frame** { **bottom** | **front-panel** | **menu** } | **hp-top-tools** | **http** | **https** | **list-menu** | **page-menu** | **page-size** *size* | **session-timeout** *time* | **tcp-port** *port-num*]

no web-management [**allow-no-password** | **connection-receive-timeout** *timeout-value* | **frame** { **bottom** | **front-panel** | **menu** } | **hp-top-tools** | **http** | **https** | **list-menu** | **page-menu** | **page-size** *size* | **session-timeout** *time* | **tcp-port** *port-num*]

web-management [**refresh** { **front-panel** | **port-statistic** | **rmon** | **stp** | **tftp** } *refresh-time*]

no web-management [**refresh** { **front-panel** | **port-statistic** | **rmon** | **stp** | **tftp** } *refresh-time*]

Command Default

Web management is enabled.

Parameters

enable

Enables web management only to clients in a specific VLAN or Ethernet interface.

vlan *vlan-id*

Specifies that web management should be enabled on the clients of the specified VLAN.

ethernet *stack/sport/slot*

Specifies the Ethernet interface on which web management should be enabled.

to *stack/sport/slot*

Specifies the range of Ethernet interfaces.

allow-no-password

Allows the web server to have no password.

connection-receive-timeout *timeout-value*

Specifies the web connection receive timeout.

frame

Enables a frame.

bottom

The bottom frame.

front-panel

The front-panel frame.

menu
The menu frame.

hp-top-tools
Enables the support of HP Top Tools.

http
Enables web management for HTTP access.

https
Enables web management for HTTPS access.

list-menu
Displays the web menu as a list.

page-menu
Enables the page menu.

page-size *size*
Configures the maximum number of entries on a page.

session-timeout *time*
Configures the web session timeout in seconds. Valid values are from 5 through 65000.

tcp-port *port-num*
Configures the HTTP port. The default port is 80.

refresh
Configures the page refresh (polling time) in seconds.

front-panel
Configures the front-panel refresh time.

port-statistic
Configures the port statistic refresh time.

rmon
Configures the RMON statistics refresh time.

stp
Configures the STP statistics refresh time.

tftp
Configures the TFTP statistics refresh time.

refresh-time
The refresh time in seconds.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the web management configurations.

Examples

The following example shows how to enable web management for HTTPS access.

```
device(config)# web-management https
```

The following example shows how to enable web management access only to clients connected to ports within port-based VLAN 10.

```
device(config)# web-management enable vlan 10
```

The following example shows how to enable web management access on a range of Ethernet interfaces.

```
device(config)# web-management enable ethernet 1/1/1 to 1/2/3
```

The following example shows how to configure the front-panel refresh time to 30 seconds.

```
device(config)# web-management refresh front-panel 30
```

webpage custom-text

Customizes the text that appears on the title bar, login button, header, and footer on the Web Authentication pages.

Syntax

webpage custom-text { **bottom** *footer* | **login-button** *button-text* | **title** *title-text* | **top** *header* }

no webpage custom-text { **bottom** *footer* | **login-button** *button-text* | **title** *title-text* | **top** *header* }

Command Default

The default header text is "Welcome to Brocade Communications, Inc. Web Authentication Homepage".

The default title bar text is "Web Authentication".

The default login button text is "Login".

The default footer text is "This network is restricted to authorized users only. Violators may be subjected to legal prosecution. Activity on this network is monitored and may be used as evidence in a court of law. Copyright <*year*> Brocade Communications, Inc."

Parameters

bottom *footer*
: Customizes the footer on a Web Authentication page. Specify up to 255 alphanumeric characters for the string.

login-button *button-text*
: Customizes the login button that appears on the bottom of the Web Authentication Login page. Enter up to 32 alphanumeric characters for the string.

title *title-text*
: Customizes the title bar that appears on all Web Authentication pages. You can specify up to 128 alphanumeric characters.

top *header*
: Customizes the header that appears on all Web Authentication pages. You can specify up to 255 alphanumeric characters.

Modes

Web Authentication configuration mode

Usage Guidelines

You can use the **show webauth** command to view the configured text for Web Authentication pages.

The **no** form of the command resets the text to the default.

Examples

The following example shows how to customize the text on the title bar.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webpage custom-text title "Brocade Secure Access Page"
```

The following example shows how to customize the header that appears on all Web Authentication pages.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webpage custom-text top "Welcome to Network One"
```

The following example shows how to customize the login button that appears on the bottom of the Web Authentication Login page.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webpage custom-text login-button "Press to Log In"
```

The following example shows how to customize the footer that appears on all Web Authentication pages.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webpage custom-text bottom "Network One Copyright 2010"
```

webpage logo

Customizes the logo that appears on all Web Authentication pages and its placement.

Syntax

webpage logo { **copy tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **align** { **left** | **center** | **right** } }

no webpage logo [**copy tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **align** [**left** | **center** | **right**]]

Command Default

By default, the logo is left-aligned at the top of the page.

Parameters

copy tftp
: Copies an image from the TFTP server to the switch.

ipv4-address
: Specifies the IPv4 address of the TFTP server.

ipv6-address
: Specifies the IPv6 address of the TFTP server.

file-name
: Specifies the name of the file that must be copied from the TFTP server to the switch.

align
: Configures the placement of the logo on the Web Authentication pages.

  left
  : Aligns the logo to the left at the top of the page.

  right
  : Aligns the logo to the right at the top of the page.

  center
  : Aligns the logo to the center at the top of the page.

Modes

Web Authentication configuration mode

Usage Guidelines

To customize the banner image, use TFTP to upload an image file from a TFTP server to the FastIron switch. The image file can be in the jpg, bmp, or gif format, and its file size must be 64 KB or less. When you upload a new image file, it willl overwrite the existing image file.

The **no** form of the command deletes the logo from all Web Authentication pages and removes it from flash memory.

NOTE
The **webpage logo** command downloads the image file and stores it in the device flash memory. Therefore, it is not necessary to follow this command with a **write memory** command.

Examples

The following example shows how to replace the existing logo with a new one.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webpage logo copy tftp 10.10.5.1 brocadelogo.gif
```

The following example shows how to right-justify the log at the top of the page.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webpage logo align right
```

webpage terms

Customizes the text box that appears on the Web Authentication Login page.

Syntax

webpage terms copy tftp { *ipv4-address* | *ipv6-address* } *file-name*

no webpage terms copy tftp { *ipv4-address* | *ipv6-address* } *file-name*

Command Default

By default, the text box is empty and is not visible.

Parameters

copy tftp

Copies an ASCII text file from a TFTP server to the switch.

ipv4-address

The IPv4 address of the TFTP server.

ipv6-address

The IPv4 address of the TFTP server.

file-name

Specifies the name of the text file on the TFTP server.

Modes

Web Authentication configuration mode

Usage Guidelines

The text file size must not exceed 2 KB.

NOTE
The **webpage terms** command downloads the text file and stores it in the device flash memory. Therefore, it is not necessary to follow this command with a **write memory** command.

The **no** form of the command reverts back to the default; that is, the textbox is empty and not visible.

Examples

The following example shows how to create or replace a text box.

```
device(config)# vlan 10
device(config-vlan-10)# webauth
device(config-vlan-10-webauth)# webpage terms copy tftp 10.10.5.1 policy.txt
```

write terminal

Displays the running configuration.

Syntax

write terminal

Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Usage Guidelines

The command performs the same function as the **show running-config** command.

Examples

The following example shows how to execute the **write terminal** command.

```
device(config)# write terminal
Current configuration:
!
ver 08.0.30
!
stack unit 1
  module 1 icx7450-24-port-management-module
  module 2 icx7400-xgf-4port-40g-module
  module 3 icx7400-qsfp-1port-40g-module
  module 4 icx7400-qsfp-1port-40g-module
!
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 name IP_IPX_Protocol by port
!
vlan 10 by port
!
authentication
 disable-aging
!
boot sys fl sec
ip address 10.25.224.197 255.255.255.0 dynamic
ip dns domain-list englab.brocade.com
ip dns server-address 10.31.2.10
ip default-gateway 10.25.224.1
!
!
ntp
!
!
dot1x-mka-enable
!
!
sflow sample 566
sflow polling-interval 30
sflow max-packet-size 1200
sflow export cpu-traffic 18
sflow export system-info 30
sflow destination 2.2.2.2
sflow destination 3.3.3.3
sflow destination 4.4.4.4
sflow source-port 9999
sflow enable
!
!
end
```

xwindow-manager

Specifies the IP addresses of systems that are running the X Window System Display Manager and are available to the client.

Syntax

xwindow-manager *ip-address* [*ip-address*] [*ip-address*]

no xwindow-manager *ip-address* [*ip-address*] [*ip-address*]

Parameters

ip-address

Specifies the IP address of the system running the X Window System Display Manager.

Modes

DHCP server pool configuration mode

Usage Guidelines

You can configure a maximum of three X Window System Display Manager IP addresses in a DHCP server pool.

The **no** form of the command removes the X Window System Display Manager IP addresses from the DHCP server pool.

Examples

The following example configures the IP addresses of systems that are running the X Window System Display Manager in a DHCP server pool.

```
device(config)# ip dhcp-server pool cabo
device(config-dhcp-cabo)# xwindow-manager 10.38.12.1 10.38.12.3 10.38.12.5
```

History

Release version	Command history
8.0.30b	This command was introduced.



© 2022 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com