NetIron Command Line Interface (CLI) Reference Guide

Supporting NetIron OS 6.0.00
NetIron Command Line Interface (CLI) Reference Guide
# Contents

<table>
<thead>
<tr>
<th>Preface</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document conventions</td>
<td>19</td>
</tr>
<tr>
<td>Text formatting conventions</td>
<td>19</td>
</tr>
<tr>
<td>Command syntax conventions</td>
<td>19</td>
</tr>
<tr>
<td>Notes, cautions, and warnings</td>
<td>20</td>
</tr>
<tr>
<td>Brocade resources</td>
<td>20</td>
</tr>
<tr>
<td>Contacting Brocade Technical Support</td>
<td>20</td>
</tr>
<tr>
<td>Brocade customers</td>
<td>20</td>
</tr>
<tr>
<td>Brocade OEM customers</td>
<td>21</td>
</tr>
<tr>
<td>Document feedback</td>
<td>21</td>
</tr>
<tr>
<td>About This Document</td>
<td>23</td>
</tr>
<tr>
<td>What’s new in this document</td>
<td>23</td>
</tr>
<tr>
<td>New commands</td>
<td>23</td>
</tr>
<tr>
<td>Modified commands</td>
<td>24</td>
</tr>
<tr>
<td>Deprecated commands</td>
<td>25</td>
</tr>
<tr>
<td>Supported hardware and software</td>
<td>25</td>
</tr>
<tr>
<td>Using the Netiron Command-Line Interface</td>
<td>27</td>
</tr>
<tr>
<td>Logging on through the CLI</td>
<td>27</td>
</tr>
<tr>
<td>On-line help</td>
<td>27</td>
</tr>
<tr>
<td>Command completion</td>
<td>28</td>
</tr>
<tr>
<td>Scroll control</td>
<td>28</td>
</tr>
<tr>
<td>Line editing commands</td>
<td>28</td>
</tr>
<tr>
<td>Command configuration modes</td>
<td>29</td>
</tr>
<tr>
<td>User EXEC mode</td>
<td>29</td>
</tr>
<tr>
<td>Privileged EXEC mode</td>
<td>29</td>
</tr>
<tr>
<td>Global configuration mode</td>
<td>29</td>
</tr>
<tr>
<td>Configuration modes</td>
<td>29</td>
</tr>
<tr>
<td>Accessing the CLI</td>
<td>30</td>
</tr>
<tr>
<td>Single user in global configuration mode</td>
<td>31</td>
</tr>
<tr>
<td>Multi-user conflict during deletion of group configuration (or stanza)</td>
<td>32</td>
</tr>
<tr>
<td>Navigating among command levels</td>
<td>32</td>
</tr>
<tr>
<td>CLI command structure</td>
<td>32</td>
</tr>
<tr>
<td>Required or optional fields</td>
<td>33</td>
</tr>
<tr>
<td>Optional fields</td>
<td>33</td>
</tr>
<tr>
<td>List of available options</td>
<td>33</td>
</tr>
<tr>
<td>Searching and filtering output</td>
<td>33</td>
</tr>
<tr>
<td>Searching and filtering output from show commands</td>
<td>34</td>
</tr>
<tr>
<td>Searching and filtering output at the --More-- prompt</td>
<td>35</td>
</tr>
<tr>
<td>Using special characters in regular expressions</td>
<td>36</td>
</tr>
<tr>
<td>Allowable characters for LAG names</td>
<td>38</td>
</tr>
<tr>
<td>CLI parsing enhancement</td>
<td>39</td>
</tr>
<tr>
<td>Syntax shortcuts</td>
<td>39</td>
</tr>
<tr>
<td>Saving configuration changes</td>
<td>39</td>
</tr>
<tr>
<td>Modifying startup and running configuration file manually</td>
<td>39</td>
</tr>
<tr>
<td>Commands A - E</td>
<td>41</td>
</tr>
</tbody>
</table>
clear bm histogram ..........................................................116
clear cpu histogram sequence ...........................................117
clear dot1x-mka statistics..................................................118
clear ikev2 statistics .......................................................119
clear ikev2 sa ....................................................................120
clear ip bgp dampening ....................................................121
clear ip bgp flap-statistics ................................................122
clear ip bgp local routes ....................................................123
clear ip bgp neighbor ......................................................124
clear ip bgp routes ..........................................................126
clear ip bgp traffic ............................................................127
clear ip bgp vrf .................................................................128
clear ip vrrp statistics ......................................................129
clear ip vrrp-extended statistics .......................................130
clear ipsec error-count ....................................................131
clear ipsec sa .................................................................132
clear ipsec statistics .......................................................133
clear ipsec statistics tunnel ..............................................134
clear ipv6 bgp dampening ...............................................135
clear ipv6 bgp flap-statistics ..........................................136
clear ipv6 bgp local routes ...............................................137
clear ipv6 bgp neighbor ...................................................138
clear ipv6 bgp routes ......................................................140
clear ipv6 bgp traffic .......................................................141
clear ipv6 vrrp statistics ................................................142
clear ipv6 vrrp-extended statistics ...................................143
clear isis shortcut ..........................................................144
clear macsec statistics ....................................................145
clear memory histogram ..................................................146
clear metro mp-vlp-queue ..............................................147
clear mpls auto-bandwidth-samples ................................148
clear mpls ldp neighbor ..................................................149
clear mpls ldp statistics ..................................................151
clear mpls rsvp statistics session ....................................152
clear mpls statistics ........................................................154
clear openflow ..............................................................157
clear pki counters ..........................................................158
clear pki crl .................................................................159
clear rate-limit counters bum-drop .................................160
clear rate-limit counters ip-option-pkt-to-cpu ..................161
clear rate-limit counters ipv6-hoplimit-expired-to-cpu ....162
clear rate-limit counters ip-ttl-expired-to-cpu .................163
clear statistics openflow ...............................................164
client-interfaces sync_ccp_early ....................................165
cluster-client-static-mac-move ......................................166
cluster-id ......................................................................167
copy .................................................................168
copy tftp license ...........................................................170
copy-received-cos .........................................................171
common-name .............................................................172
ipv6 route next-hop........................................................................................................................................................................................................................................................................361
ipv6 route next-hop-enable-default........................................................................................................................................................................................................................................................................362
ipv6 next-hop-recursion........................................................................................................................................................................................................................................................................363
ipv6 route static-bfd........................................................................................................................................................................................................................................................................364
ipv6 router ospf........................................................................................................................................................................................................................................................................366
ipv6 router vrrp........................................................................................................................................................................................................................................................................367
ipv6 router vrrp-extended........................................................................................................................................................................................................................................................................368
ipv6 traffic-filter........................................................................................................................................................................................................................................................................369
ipv6 traffic-filter enable-deny-logging........................................................................................................................................................................................................................................................................371
ipv6 vrrp vrid........................................................................................................................................................................................................................................................................373
ipv6 vrrp-extended vrid........................................................................................................................................................................................................................................................................374
isis bfd........................................................................................................................................................................................................................................................................375
isis reverse-metric........................................................................................................................................................................................................................................................................376
jtc enable........................................................................................................................................................................................................................................................................379

Commands K - Sh........................................................................................................................................................................................................................................................................381
key-add-remove-interval........................................................................................................................................................................................................................................................................381
key-rollover-interval........................................................................................................................................................................................................................................................................382
key-server-priority........................................................................................................................................................................................................................................................................383
l2 policy route-map........................................................................................................................................................................................................................................................................384
label-range static........................................................................................................................................................................................................................................................................386
label-withdrawal-delay........................................................................................................................................................................................................................................................................387
License add........................................................................................................................................................................................................................................................................388
license delete........................................................................................................................................................................................................................................................................389
link-protection........................................................................................................................................................................................................................................................................390
local-as........................................................................................................................................................................................................................................................................391
load-balance mask ip........................................................................................................................................................................................................................................................................392
load-balance mask ipv6........................................................................................................................................................................................................................................................................394
local-certificate........................................................................................................................................................................................................................................................................396
location........................................................................................................................................................................................................................................................................397
log (OSPFv2)........................................................................................................................................................................................................................................................................398
logging enable........................................................................................................................................................................................................................................................................400
log-dampening-debug........................................................................................................................................................................................................................................................................403
log-status-change........................................................................................................................................................................................................................................................................404
logs-per-interval-per-mep-rnep........................................................................................................................................................................................................................................................................405
lsr-id........................................................................................................................................................................................................................................................................406
mac access-group........................................................................................................................................................................................................................................................................407
mac access-group enable-deny-logging........................................................................................................................................................................................................................................................................409
mac access-list........................................................................................................................................................................................................................................................................410
mac-age-time........................................................................................................................................................................................................................................................................412
mac-move-det-syslog........................................................................................................................................................................................................................................................................414
macsec cipher-suite........................................................................................................................................................................................................................................................................416
macsec confidentiality-offset........................................................................................................................................................................................................................................................................418
macsec frame-validation........................................................................................................................................................................................................................................................................420
macsec replay-protection........................................................................................................................................................................................................................................................................421
match additional paths advertise-set........................................................................................................................................................................................................................................................................422
match identity........................................................................................................................................................................................................................................................................424
match l2acl........................................................................................................................................................................................................................................................................426
med-missing-as-worst........................................................................................................................................................................................................................................................................427
method........................................................................................................................................................................................................................................................................428
metric-type........................................................................................................................................................................................................................................................................429
show egress-truncate.......................................................................................................................583
show ikev2 policy..........................................................................................................................584
show ikev2 profile......................................................................................................................585
show ikev2 proposal.....................................................................................................................586
show ikev2 sa..............................................................................................................................587
show ikev2 session......................................................................................................................589
show ikev2 statistics....................................................................................................................591
show interface ethernet..............................................................................................................593
show interfaces tunnel..............................................................................................................595
show ip allow-src-multicast......................................................................................................597
show ip bgp..................................................................................................................................598
show ip bgp attribute-entries......................................................................................................599
show ip bgp config......................................................................................................................601
show ip bgp dampened-paths......................................................................................................602
show ip bgp filtered-routes.......................................................................................................603
show ip bgp flap-statistics.........................................................................................................604
show ip bgp ipv6 ..........................................................................................................................606
show ip bgp neighbors..............................................................................................................609
show ip bgp neighbors advertised-routes..................................................................................616
show ip bgp neighbors flap-statistics......................................................................................617
show ip bgp neighbors last-packet-with-error .........................................................................618
show ip bgp neighbors received-routes ...................................................................................619
show ip bgp neighbors received-routes ...................................................................................620
show ip bgp neighbors rib-out-routes ......................................................................................621
show ip bgp routes community ...............................................................................................622
show ip bgp routes community ...............................................................................................623
show ip bgp routes community ...............................................................................................624
show ip bgp peer-group .............................................................................................................627
show ip bgp routes ....................................................................................................................628
show ip bgp summary ................................................................................................................632
show ip bgp vrf neighbors ........................................................................................................635
show ip bgp vrf routes ..............................................................................................................637
show ip bgp vrf ..........................................................................................................................639
show ip http client.....................................................................................................................641
show ip interface .......................................................................................................................643
show ip mbgp ipv6 .....................................................................................................................647
show ip multicast.......................................................................................................................649
show ip multicast vpls................................................................................................................653
show ip ospf...............................................................................................................................656
show ip route............................................................................................................................657
show ip static-arp......................................................................................................................660
show ip vrp.................................................................................................................................662
show ip vrrp-extended...............................................................................................................665
show ipsec egress-config.........................................................................................................670
show ipsec egress-spi-table.......................................................................................................671
show ipsec error-count..............................................................................................................672
show ipsec ingress-config.........................................................................................................673
show ipsec ingress-spi-table......................................................................................................674
show ipsec policy.......................................................................................................................675
show ipsec profile......................................................................................................................676
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipsec proposal</td>
<td>678</td>
</tr>
<tr>
<td>show ipsec sa</td>
<td>680</td>
</tr>
<tr>
<td>show ipsec statistics</td>
<td>682</td>
</tr>
<tr>
<td>show ip-tunnels</td>
<td>684</td>
</tr>
<tr>
<td>show ipv6 access-list bindings</td>
<td>686</td>
</tr>
<tr>
<td>show ipv6 access-list receive accounting</td>
<td>687</td>
</tr>
<tr>
<td>show ipv6 bgp</td>
<td>688</td>
</tr>
<tr>
<td>show ipv6 bgp neighbors</td>
<td>690</td>
</tr>
<tr>
<td>show ipv6 bgp routes</td>
<td>692</td>
</tr>
<tr>
<td>show ipv6 bgp summary</td>
<td>696</td>
</tr>
<tr>
<td>show ipv6 dhcp-relay interface</td>
<td>699</td>
</tr>
<tr>
<td>show ipv6 dhcp-relay options</td>
<td>700</td>
</tr>
<tr>
<td>show ipv6 interface tunnel</td>
<td>701</td>
</tr>
<tr>
<td>show ipv6 ospf interface</td>
<td>703</td>
</tr>
<tr>
<td>show ipv6 vrrp</td>
<td>709</td>
</tr>
<tr>
<td>show ipv6 vrrp-extended</td>
<td>713</td>
</tr>
<tr>
<td>show isis</td>
<td>717</td>
</tr>
<tr>
<td>show isis shortcut</td>
<td>722</td>
</tr>
<tr>
<td>show license</td>
<td>724</td>
</tr>
<tr>
<td>show load-balance mask-options</td>
<td>726</td>
</tr>
<tr>
<td>show macsec ethernet</td>
<td>728</td>
</tr>
<tr>
<td>show macsec statistics ethernet</td>
<td>729</td>
</tr>
<tr>
<td>show memory histogram</td>
<td>732</td>
</tr>
<tr>
<td>show metro mp-vlp-queue</td>
<td>734</td>
</tr>
<tr>
<td>show metro-ring</td>
<td>736</td>
</tr>
<tr>
<td>show mmrp</td>
<td>739</td>
</tr>
<tr>
<td>show mmrp attributes</td>
<td>741</td>
</tr>
<tr>
<td>show mmrp config</td>
<td>743</td>
</tr>
<tr>
<td>show mmrp statistics</td>
<td>744</td>
</tr>
<tr>
<td>show mpls autobw-threshold-table</td>
<td>746</td>
</tr>
<tr>
<td>show mpls bypass-lsp</td>
<td>747</td>
</tr>
<tr>
<td>show mpls config</td>
<td>750</td>
</tr>
<tr>
<td>show mpls forwarding</td>
<td>753</td>
</tr>
<tr>
<td>show mpls interface</td>
<td>755</td>
</tr>
<tr>
<td>show mpls label-range</td>
<td>757</td>
</tr>
<tr>
<td>show mpls ldp</td>
<td>759</td>
</tr>
<tr>
<td>show mpls ldp database</td>
<td>760</td>
</tr>
<tr>
<td>show mpls ldp fec</td>
<td>762</td>
</tr>
<tr>
<td>show mpls ldp interface</td>
<td>766</td>
</tr>
<tr>
<td>show mpls ldp neighbor</td>
<td>768</td>
</tr>
<tr>
<td>show mpls ldp path</td>
<td>770</td>
</tr>
<tr>
<td>show mpls ldp peer</td>
<td>772</td>
</tr>
<tr>
<td>show mpls ldp session</td>
<td>774</td>
</tr>
<tr>
<td>show mpls ldp statistics</td>
<td>776</td>
</tr>
<tr>
<td>show mpls ldp tunnel</td>
<td>778</td>
</tr>
<tr>
<td>show mpls lsp</td>
<td>780</td>
</tr>
<tr>
<td>show mpls lsp_p2mp_xc</td>
<td>787</td>
</tr>
<tr>
<td>show mpls path</td>
<td>789</td>
</tr>
<tr>
<td>show mpls policy</td>
<td>791</td>
</tr>
<tr>
<td>show mpls route</td>
<td>794</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>show mpls rsvp interface</td>
<td>796</td>
</tr>
<tr>
<td>show mpls rsvp neighbor</td>
<td>798</td>
</tr>
<tr>
<td>show mpls rsvp session</td>
<td>801</td>
</tr>
<tr>
<td>show mpls rsvp session backup</td>
<td>806</td>
</tr>
<tr>
<td>show mpls rsvp session brief</td>
<td>808</td>
</tr>
<tr>
<td>show mpls rsvp session bypass</td>
<td>811</td>
</tr>
<tr>
<td>show mpls rsvp session detail</td>
<td>813</td>
</tr>
<tr>
<td>show mpls rsvp session detour</td>
<td>815</td>
</tr>
<tr>
<td>show mpls rsvp session down</td>
<td>820</td>
</tr>
<tr>
<td>show mpls rsvp session extensive</td>
<td>822</td>
</tr>
<tr>
<td>show mpls rsvp session (ingress/egress)</td>
<td>825</td>
</tr>
<tr>
<td>show mpls rsvp session (interface)</td>
<td>827</td>
</tr>
<tr>
<td>show mpls rsvp session name</td>
<td>828</td>
</tr>
<tr>
<td>show mpls rsvp session p2mp</td>
<td>832</td>
</tr>
<tr>
<td>show mpls rsvp session p2p</td>
<td>836</td>
</tr>
<tr>
<td>show mpls rsvp session ppend</td>
<td>838</td>
</tr>
<tr>
<td>show mpls rsvp session transit</td>
<td>840</td>
</tr>
<tr>
<td>show mpls rsvp session up</td>
<td>842</td>
</tr>
<tr>
<td>show mpls rsvp session wide</td>
<td>844</td>
</tr>
<tr>
<td>show mpls rsvp session down</td>
<td>846</td>
</tr>
<tr>
<td>show mpls static-lsp</td>
<td>848</td>
</tr>
<tr>
<td>show mpls static 6pe</td>
<td>851</td>
</tr>
<tr>
<td>show mpls statistics bypass-lsp</td>
<td>852</td>
</tr>
<tr>
<td>show mpls statistics label</td>
<td>853</td>
</tr>
<tr>
<td>show mpls statistics ldp transit</td>
<td>855</td>
</tr>
<tr>
<td>show mpls statistics ldp tunnel</td>
<td>857</td>
</tr>
<tr>
<td>show mpls statistics lsp</td>
<td>858</td>
</tr>
<tr>
<td>show mpls statistics oam</td>
<td>859</td>
</tr>
<tr>
<td>show mpls statistics vll</td>
<td>860</td>
</tr>
<tr>
<td>show mpls statistics vll-local</td>
<td>862</td>
</tr>
<tr>
<td>show mpls statistics vpls</td>
<td>864</td>
</tr>
<tr>
<td>show mpls statistics vrf</td>
<td>866</td>
</tr>
<tr>
<td>show mpls summary</td>
<td>867</td>
</tr>
<tr>
<td>show mpls ted database</td>
<td>869</td>
</tr>
<tr>
<td>show mpls ted path</td>
<td>871</td>
</tr>
<tr>
<td>show mpls vll</td>
<td>874</td>
</tr>
<tr>
<td>show mpls vll-local</td>
<td>877</td>
</tr>
<tr>
<td>show mpls vpls</td>
<td>879</td>
</tr>
<tr>
<td>show mstp</td>
<td>885</td>
</tr>
<tr>
<td>show mvrp</td>
<td>886</td>
</tr>
<tr>
<td>show mvrp attributes</td>
<td>887</td>
</tr>
<tr>
<td>show mvrp config</td>
<td>889</td>
</tr>
<tr>
<td>show mvrp statistics</td>
<td>890</td>
</tr>
<tr>
<td>show nht-table ipsec-based</td>
<td>892</td>
</tr>
<tr>
<td>show openflow</td>
<td>893</td>
</tr>
<tr>
<td>show openflow controller</td>
<td>895</td>
</tr>
<tr>
<td>show openflow flows</td>
<td>896</td>
</tr>
<tr>
<td>show openflow groups</td>
<td>898</td>
</tr>
<tr>
<td>show openflow interface</td>
<td>900</td>
</tr>
</tbody>
</table>
show openflow meters.......................................................................................................................901
show openflow queues.......................................................................................................................903
show pim interface .......................................................................................................................905
show pim multicast-filter.......................................................................................................................906
show pki certificates.......................................................................................................................907
show pki counters.......................................................................................................................910
show pki crls.............................................................................................................................................................................................................911
show pki enrollment-profile.......................................................................................................................912
show pki entity.......................................................................................................................................................................................913
show pki key mypubkey.......................................................................................................................................................................................914
show pki trustpoint.......................................................................................................................................................................................915
show rate-limit counters bum-drop...................................................................................................................................................................................................917
show rate-limit counters ipv6 hop-limit-expired-to-cpu.........................................................................................................................................................................................................919
show rate-limit interface................................................................................................................................................................................................................920
show rate-limit ipv6 hop-limit-expired-to-cpu.............................................................................................................................................................................................................921
show rate-limit option-pkt-to-cpu.............................................................................................................................................................................................................922
show rate-limit ttl-expired-to-cpu.............................................................................................................................................................................................................923
show rmon alarm.......................................................................................................................................................................................924
show rmon statistics.............................................................................................................................................................................................................925
show route-map.............................................................................................................................................................................................................927
show rstp .............................................................................................................................................................................................................928
show running-config.............................................................................................................................................................................................................930
show sflow statistics .............................................................................................................................................................................................................932
show spanning-tree.............................................................................................................................................................................................................933
show statistics.............................................................................................................................................................................................................935
show sysmon config.............................................................................................................................................................................................................939
show sysmon results brief.............................................................................................................................................................................................................940
show sysmon results detail.............................................................................................................................................................................................................942
show sysmon schedule.............................................................................................................................................................................................................944
show telemetry.............................................................................................................................................................................................................946
show terminal.............................................................................................................................................................................................................947
show tm-voq-stat queue-drops.............................................................................................................................................................................................................948
show tvf-domain.............................................................................................................................................................................................................949
show vlan.............................................................................................................................................................................................................953
show vlan tvf-lag-ib.............................................................................................................................................................................................................955
Commands Si - Z.............................................................................................................................................................................................................957

slow-start.............................................................................................................................................................................................................957
snmp-server community.............................................................................................................................................................................................................959
snmp-server context .............................................................................................................................................................................................................961
snmp-server enable mib.............................................................................................................................................................................................................962
snmp-server enable traps.............................................................................................................................................................................................................963
snmp-server enable traps bum-rl-traps.............................................................................................................................................................................................................964
snmp-server host.............................................................................................................................................................................................................965
snmp-server mib community-map.............................................................................................................................................................................................................968
spanning-tree pvst-protect.............................................................................................................................................................................................................969
state-name.............................................................................................................................................................................................................971
static-lsp.............................................................................................................................................................................................................972
static-mac-address.............................................................................................................................................................................................................973
statistics-load-interval.............................................................................................................................................................................................................974
subject-alt-name.............................................................................................................................................................................................................976
<table>
<thead>
<tr>
<th>Command Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary-address (OSPFv3)</td>
<td>977</td>
</tr>
<tr>
<td>suppress-acl-seq</td>
<td>979</td>
</tr>
<tr>
<td>suppress-ipv6-priority-mapping</td>
<td>980</td>
</tr>
<tr>
<td>sysmon fe link auto-tune</td>
<td>981</td>
</tr>
<tr>
<td>sysmon ipc rel-q-mon enable</td>
<td>982</td>
</tr>
<tr>
<td>sysmon lp-high-cpu enable</td>
<td>983</td>
</tr>
<tr>
<td>sysmon lp-high-cpu threshold</td>
<td>984</td>
</tr>
<tr>
<td>sysmon mp-high-cpu cpu-threshold</td>
<td>985</td>
</tr>
<tr>
<td>sysmon mp-high-cpu enable</td>
<td>986</td>
</tr>
<tr>
<td>sysmon mp-high-cpu task-threshold</td>
<td>987</td>
</tr>
<tr>
<td>sysmon np memory-errors</td>
<td>988</td>
</tr>
<tr>
<td>sysmon port port-crc-test</td>
<td>989</td>
</tr>
<tr>
<td>sysmon sfm walk auto</td>
<td>993</td>
</tr>
<tr>
<td>sysmon sfm walk polling-period</td>
<td>994</td>
</tr>
<tr>
<td>sysmon sfm walk redundancy-check</td>
<td>995</td>
</tr>
<tr>
<td>sysmon sfm walk start</td>
<td>996</td>
</tr>
<tr>
<td>sysmon sfm walk status</td>
<td>997</td>
</tr>
<tr>
<td>sysmon sfm walk stop</td>
<td>998</td>
</tr>
<tr>
<td>sysmon sfm walk threshold</td>
<td>1000</td>
</tr>
<tr>
<td>sysmon tm link auto-tune</td>
<td>1002</td>
</tr>
<tr>
<td>system np control-ram-threshold</td>
<td>1003</td>
</tr>
<tr>
<td>system np ipm-ram-threshold</td>
<td>1005</td>
</tr>
<tr>
<td>system-init</td>
<td>1007</td>
</tr>
<tr>
<td>system-max ecmp-pram-block-size</td>
<td>1009</td>
</tr>
<tr>
<td>system-max ip-arp</td>
<td>1010</td>
</tr>
<tr>
<td>system-max ipv6-receive-cam</td>
<td>1011</td>
</tr>
<tr>
<td>system-max ipv6-vrf-route</td>
<td>1012</td>
</tr>
<tr>
<td>system-max ip-vrf-route</td>
<td>1013</td>
</tr>
<tr>
<td>system-max rstp</td>
<td>1014</td>
</tr>
<tr>
<td>system-max trunk-num</td>
<td>1015</td>
</tr>
<tr>
<td>system-max tvf-lag-lb-fid-group</td>
<td>1016</td>
</tr>
<tr>
<td>system-max tvf-lag-lb-fid-pool</td>
<td>1017</td>
</tr>
<tr>
<td>te-metric</td>
<td>1018</td>
</tr>
<tr>
<td>terminal enable timestamp</td>
<td>1019</td>
</tr>
<tr>
<td>timers (OSPFv3)</td>
<td>1022</td>
</tr>
<tr>
<td>traceroute</td>
<td>1024</td>
</tr>
<tr>
<td>traceroute mpls ldp</td>
<td>1026</td>
</tr>
<tr>
<td>track-port</td>
<td>1028</td>
</tr>
<tr>
<td>transparent-hw-flooding lag-load-balancing</td>
<td>1030</td>
</tr>
<tr>
<td>tunnel destination</td>
<td>1031</td>
</tr>
<tr>
<td>tunnel mode ipsec ipv4</td>
<td>1032</td>
</tr>
<tr>
<td>tunnel mode ipsec ipv6</td>
<td>1033</td>
</tr>
<tr>
<td>tunnel override-pkt-tos-ttl</td>
<td>1034</td>
</tr>
<tr>
<td>tunnel protection ipsec profile</td>
<td>1035</td>
</tr>
<tr>
<td>tunnel source</td>
<td>1036</td>
</tr>
<tr>
<td>tunnel-interface</td>
<td>1037</td>
</tr>
<tr>
<td>tvf-domain</td>
<td>1039</td>
</tr>
<tr>
<td>uda access-group</td>
<td>1040</td>
</tr>
<tr>
<td>uda-offsets</td>
<td>1042</td>
</tr>
<tr>
<td>underflow-limit</td>
<td>1044</td>
</tr>
</tbody>
</table>
Document conventions

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

Text formatting conventions

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

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold text</strong></td>
<td>Identifies command names</td>
</tr>
<tr>
<td></td>
<td>Identifies keywords and operands</td>
</tr>
<tr>
<td></td>
<td>Identifies the names of user-manipulated GUI elements</td>
</tr>
<tr>
<td></td>
<td>Identifies text to enter at the GUI</td>
</tr>
<tr>
<td><em>italic text</em></td>
<td>Identifies emphasis</td>
</tr>
<tr>
<td></td>
<td>Identifies variables</td>
</tr>
<tr>
<td></td>
<td>Identifies document titles</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Identifies CLI output</td>
</tr>
<tr>
<td></td>
<td>Identifies command syntax examples</td>
</tr>
</tbody>
</table>

Command syntax conventions

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold text</strong></td>
<td>Identifies command names, keywords, and command options.</td>
</tr>
<tr>
<td><em>italic text</em></td>
<td>Identifies a variable.</td>
</tr>
<tr>
<td>value</td>
<td>In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, --show WWN.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Syntax components displayed within square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>x</td>
<td>y</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, for example, passwords, are enclosed in angle brackets.</td>
</tr>
</tbody>
</table>
Conventions

- 
  Repeat the previous element, for example, 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.

Notes, cautions, and warnings

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

**NOTE**

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

**ATTENTION**

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

**CAUTION**

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

**DANGER**

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

Brocade resources

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

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.
If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

<table>
<thead>
<tr>
<th>Online</th>
<th>Telephone</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preferred method of contact for non-urgent issues:</strong></td>
<td><strong>Required for Sev 1-Critical and Sev 2-High issues:</strong></td>
<td><a href="mailto:support@brocade.com">support@brocade.com</a></td>
</tr>
<tr>
<td>∙ My Cases through MyBrocade</td>
<td>∙ Continental US: 1-800-752-8061</td>
<td>Please include:</td>
</tr>
<tr>
<td>∙ Software downloads and licensing tools</td>
<td>∙ Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)</td>
<td>∙ Problem summary</td>
</tr>
<tr>
<td>∙ Knowledge Base</td>
<td>∙ For areas unable to access toll free number: +1-408-333-6061</td>
<td>∙ Serial number</td>
</tr>
<tr>
<td></td>
<td>∙ Toll-free numbers are available in many countries.</td>
<td>∙ Installation details</td>
</tr>
<tr>
<td></td>
<td></td>
<td>∙ Environment description</td>
</tr>
</tbody>
</table>

**Brocade OEM customers**

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

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

**Document feedback**

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

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

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

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.
What’s new in this document

This document is the NetIron Command Reference.

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

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

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

New commands

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

- additional-paths
- additional-paths select
- advertise-best-external
- clear np qos statistics
- client-interfaces sync_ccep_early
- dead-timer
- disable-acl-for-6to4
- disable-acl-for-gre
- enable pce
- enable-qos-statistics
- match additional-paths advertise-set
- message-bundle-support
- max-unknown-messages
- max-unknown-requests
- min-keepalive
- negotiation-deny
- neighbor additional-paths
- neighbor additional-paths advertise
- new additional-paths disable
• pce compute
• preference
• request-timer
• router pcep
• set next-hop-tvf-domain
• show acl-policy
• show tvf-domain
• suppress-ipv6-priority-mapping
• sysmon mp-high-cpu enable
• sysmon mp-high-cpu cpu-threshold
• sysmon mp-high-cpu task-threshold
• sysmon ipc rel-q-mon enable
• tvr-domain
• vll-peer (load-balance)

Modified commands
The following commands have been modified in this release.
• ipv6 access-list
• interface ve
• set next-hop-tvf-domain
• show cluster
• show ipsec profile
• show ip multicast
• show ip multicast vpls
• show ip route
• show ipv6 bgp neighbors
• show ipv6 bgp routes
• show np qos statistics
• show mpls vll
• show run
• track-port
• vll-peer
• vll-peer (load balance)
 Deprecated commands
There are no deprecated commands in this release.

Supported hardware and software
The following hardware platforms are supported by this release of this guide:

**TABLE 1 Supported devices**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade NetIron XMR 4000</td>
<td>Brocade MLX-4</td>
<td>Brocade NetIron CES 2024C</td>
</tr>
<tr>
<td>Brocade NetIron XMR 8000</td>
<td>Brocade MLX-8</td>
<td>Brocade NetIron CES 2024F</td>
</tr>
<tr>
<td>Brocade NetIron XMR 16000</td>
<td>Brocade MLX-16</td>
<td>Brocade NetIron CES 2048C</td>
</tr>
<tr>
<td>Brocade NetIron XMR 32000</td>
<td>Brocade MLXe-4</td>
<td>Brocade NetIron CES 2048CX</td>
</tr>
<tr>
<td></td>
<td>Brocade MLXe-8</td>
<td>Brocade NetIron CES 2048F</td>
</tr>
<tr>
<td></td>
<td>Brocade MLXe-16</td>
<td>Brocade NetIron CES 2048FX</td>
</tr>
<tr>
<td></td>
<td>Brocade MLXe-32</td>
<td>Brocade NetIron CER 2024C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER-RT 2024C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER 2024F</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER-RT 2024F</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER 2048C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER-RT 2048C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER 2048CX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER-RT 2048CX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER 2048F</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER-RT 2048F</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER 2048FX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brocade NetIron CER-RT 2048FX</td>
</tr>
</tbody>
</table>
Using the NetIron Command-Line Interface

• Logging on through the CLI .................................................. 27
• Command configuration modes ........................................... 29
• CLI command structure ....................................................... 32
• Searching and filtering output ........................................... 33
• Allowable characters for LAG names .................................. 38
• CLI parsing enhancement .................................................... 39
• Syntax shortcuts .................................................................. 39
• Saving configuration changes ............................................. 39

Logging on through the CLI

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

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

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

• **User EXEC mode** - Lets you display information and perform basic tasks such as pings and traceroutes.

• **Privileged EXEC mode** - Lets you use the same commands as those at the User EXEC level plus configuration commands that do not require saving the changes to the system-config file.

• **Global configuration mode** - Lets you make configuration changes to the device. To save the changes across software reloads and system resets, you need to save them to the system-config file. The global configuration mode contains sub-configuration modes for individual ports, for VLANs, for routing protocols, and other configuration areas.

**NOTE**

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

On-line help

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

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

device(config)# rooter ip
Unrecognized command
Command completion

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

Scroll control

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

```
   aaa
  access-list
 all-client
   arp
   banner
 base-mac-addr
  boot
 some line omitted for brevity...
 default-vlan-id
   enable
 enable-acl-counter
  end
   exit
   --More--
```

The software provides the following scrolling options:

- 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 cancel the display.

Line editing commands

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

<table>
<thead>
<tr>
<th>CTRL+Key combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL+A</td>
<td>Moves to the first character on the command line.</td>
</tr>
<tr>
<td>CTRL+B</td>
<td>Moves the cursor back one character.</td>
</tr>
<tr>
<td>CTRL+C</td>
<td>Escapes and terminates command prompts and ongoing tasks (such as lengthy displays), and displays a fresh command prompt.</td>
</tr>
<tr>
<td>CTRL+D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>CTRL+E</td>
<td>Moves to the end of the current command line.</td>
</tr>
<tr>
<td>CTRL+F</td>
<td>Moves the cursor forward one character.</td>
</tr>
<tr>
<td>CTRL+K</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>CTRL+L; CTRL+R</td>
<td>Repeats the current command line on a new line.</td>
</tr>
<tr>
<td>CTRL+N</td>
<td>Enters the next command line in the history buffer.</td>
</tr>
<tr>
<td>CTRL+P</td>
<td>Enters the previous command line in the history buffer.</td>
</tr>
</tbody>
</table>
TABLE 2 CLI line editing commands (continued)

<table>
<thead>
<tr>
<th>Ctrl+Key combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+U; Ctrl+X</td>
<td>Deletes all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl+W</td>
<td>Deletes the last word you typed.</td>
</tr>
<tr>
<td>Ctrl+Z</td>
<td>Moves from any CONFIG level of the CLI to the Privileged EXEC level; at the Privileged EXEC level, moves to the User EXEC level.</td>
</tr>
</tbody>
</table>

Command configuration modes

The Brocade CLI uses an industry-standard hierarchical shell familiar to Ethernet/IP networking administrators. You can use one of three major command modes to enter commands and access sub-configuration modes on the device.

User EXEC mode

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

```
device> enable
device#
```

Privileged EXEC mode

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

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

Global configuration mode

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

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

Configuration modes

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

The following table displays a list of the most commonly-used sub-configuration modes, but this list is not exhaustive and new sub-configuration modes can be introduced with new features. Refer to the command pages for details of the configuration modes applicable to the CLI command and examples of how to access the required mode.
### TABLE 3 Sub-configuration modes

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

### Accessing the CLI

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

device>

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

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

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

```
device> enable
```

<table>
<thead>
<tr>
<th>User Level commands</th>
<th>Privileged Level-EXEC commands</th>
<th>Global Level-CONFIG commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>device # configure terminal</td>
<td>device# configure terminal</td>
<td>device(config)#</td>
</tr>
</tbody>
</table>

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

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

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

**NOTE**

The CLI prompt at the interface level includes the port speed. The speed is one of the following:

- The interface is a 10/100 port
- The interface is a Gigabit port

For simplicity, the port speeds sometimes are not shown in example Interface level prompts in this manual.

**Single user in global configuration mode**

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

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

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

**Syntax:** `[no] single-config-user`
After the `single-config-user` command is issued, the device will not allow more than one user to enter global configuration mode. However, if you run the command while more than one user is in global configuration mode, the other users continue to be in global configuration mode and can potentially override each other's configuration changes. Only users who try to enter the global configuration mode after the command is issued are prevented from entering global configuration mode. If a user is already in that mode and another user tries to enter global configuration mode after the `single-config-user` command is issued, the following error is displayed.

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

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

- `console`
- `telnet number`
- `SSH number`

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

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

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

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

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

```
Session 1:
device(config)# vlan 10
device(config-vlan-10)#
Session 2:
device(config)# no vlan 10
"Error: Cannot undo the configuration as {console|telnet|SSH} session is using this mode."
```

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

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

**NOTE**

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

**Navigating among command levels**

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

**CLI command structure**

Many CLI commands may require textual or numeral input as part of the command.
Required or optional fields
These fields are either required or optional depending on how the information is bracketed. For clarity, a few CLI command examples are explained below.

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

When an item is in italics, the information requested is a variable and required.
When an item is not bracketed with `[]` symbols, the item is a required keyword or variable.
When an item is bracketed with `{ }` symbols, one of the items separated by a vertical bar `|` must be chosen.
When an item is bracketed with `[ ]` symbols, the information requested is optional.

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

Syntax: priority normal | high

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

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

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

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

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

Enter the following to view possible copy command options.

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

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

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

Displaying lines containing a specified string

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

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

Syntax: `show-command include | regular-expression`

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

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

Displaying lines that do not contain a specified string

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

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

Syntax: `show-command exclude | regular-expression`

Displaying lines starting with a specified string

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

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

Syntax: `show-command begin | regular-expression`
Searching and filtering output at the --More-- prompt

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

```
device# ?
```

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

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

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

The results of the search are displayed.

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

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

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

The filtered results are displayed.

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

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

```
--More--, next page: Space, next line: Return key, quit: Control-c
-telnet
```
The filtered results are displayed.

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

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

Using special characters in regular expressions

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

<table>
<thead>
<tr>
<th>Character</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>The period matches on any single character, including a blank space. For example, the following regular expression matches &quot;aaz&quot;, &quot;abz&quot;, &quot;acz&quot;, and so on, but not just &quot;az&quot;: a.z</td>
</tr>
<tr>
<td>*</td>
<td>The asterisk matches on zero or more sequential instances of a pattern. For example, the following regular expression matches output that contains the string &quot;abc&quot;, followed by zero or more Xs: abcX*</td>
</tr>
<tr>
<td>+</td>
<td>The plus sign matches on one or more sequential instances of a pattern. For example, the following regular expression matches output that contains &quot;de&quot;, followed by a sequence of &quot;g&quot;s, such as &quot;deg&quot;, &quot;degg&quot;, &quot;deggg&quot;, and so on: deg+</td>
</tr>
<tr>
<td>?</td>
<td>The question mark matches on zero occurrences or one occurrence of a pattern. For example, the following regular expression matches output that contains &quot;dg&quot; or &quot;deg&quot;: de?g</td>
</tr>
<tr>
<td>^</td>
<td>A caret (when not used within brackets) matches on the beginning of an input string.</td>
</tr>
</tbody>
</table>

**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.
### TABLE 4 Special characters for regular expressions (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>For example, the following regular expression matches output that begins with “deg”: ^deg</td>
</tr>
<tr>
<td>$</td>
<td>A dollar sign matches on the end of an input string. For example, the following regular expression matches output that ends with “deg”: deg$</td>
</tr>
</tbody>
</table>
| _         | An underscore matches on one or more of the following:  
  ∙ , (comma)  
  ∙ { (left curly brace)  
  ∙ ) (right curly brace)  
  ∙ ( (left parenthesis)  
  ∙ ) (right parenthesis)  
  ∙ The beginning of the input string  
  ∙ The end of the input string  
  ∙ A blank space  
For example, the following regular expression matches on “100” but not on “1002”, “2100”, and so on. _100_ |
| [ ]       | Square brackets enclose a range of single-character patterns. For example, the following regular expression matches output that contains “1”, “2”, “3”, “4”, or “5”: [1-5]  
You can use the following expression symbols within the brackets. These symbols are allowed only inside the brackets.  
  ∙ ^ - The caret matches on any characters except the ones in the brackets. For example, the following regular expression matches output that does not contain “1”, “2”, “3”, “4”, or “5”: [^1-5]  
  ∙ - The hyphen separates the beginning and ending of a range of characters. A match occurs if any of the characters within the range is present. See the example above. |
| | A vertical bar separates two alternative values or sets of values. The output can match one or the other value. For example, the following regular expression matches output that contains either “abc” or “defg”: abc|defg |
| ()        | Parentheses allow you to create complex expressions. For example, the following complex expression matches on “abc”, “abcabc”, or “defg”, but not on “abcdefgdefg”: ((abc+)|(defg)?) |
If you want to filter for a special character instead of using the special character as described in the table above, enter \ (backslash) in front of the character. For example, to filter on output containing an asterisk, enter the asterisk portion of the regular expression as \*.

device#show ip route bgp | include \*

Allowable characters for LAG names

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

The following characters are valid in file names:

- All upper and lowercase letters
- All digits

Any of the following special characters are valid:

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

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

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

Syntax shortcuts

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

Saving configuration changes

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

This approach in adopting configuration changes:

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

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

**NOTE**

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

Modifying startup and running configuration file manually

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

**NOTE**

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

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

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

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

No access list is created.

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

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

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

`vlan vlan-id` Indicates the selected VLAN.

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

`ipv6-source-prefix wildcard-mask` Lets the user specify a group of source destination IPv6 addresses. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

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

`host` The `host ipv6-source-address` and `host ipv6-destination-address` parameter lets you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.
Specifies a source or destination prefix and prefix length that a packet must match for the specified deny or permit action to occur. The user must specify the `ipv6-source-prefix` and `ipv6-destination-prefix` parameters in hexadecimal using 16-bit values between colons, as documented in RFC 2373. The user must specify the `prefix-length` parameter as a decimal value. A slash (/) must follow the `ipv6-prefix` parameter and precede the `prefix-length` parameter.

`ipv6-destination-prefix wildcard-mask`

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

`any`

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

`host`

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

`ipv6-destination-address`

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

`ipv6-operator value`

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

`copy-sflow`

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

`drop-precedence dp-value`

Sets the drop precedence by the selected value.

`drop-precedence-force dp-value`

Sets the force drop precedence by the selected value.

`dscp dscp-value`

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

`dscp-marking dscp-value`

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

`mirror`

Mirrors packets matching to the ACL permit clause.

`priority-force number`

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

`regenerate-seq-num dec`

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

Global configuration mode

You can also create ACLs using the following commands:

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

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

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

```plaintext
device# configure terminal
device(config)# access-list 400 deny any any any etype arp
device(config)# access-list 400 deny any any any etype ipv6
device(config)# access-list 400 deny any any any etype 8848
device(config)# access-list 400 permit any any 100
device(config)# interface ethernet 4/12
device(config-int-e100-4/12)# mac access-group 400 in
```

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

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

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

```plaintext
device# configure terminal
device(config)# access-list 101 deny tcp host 10.157.22.26 any eq telnet
device(config)# access-list 101 permit ip any any
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group 1 in
```

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was modified to include the dscp-marking dscp-value parameter.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the ipv6_destination_prefix wildcard-mask and ipv6-source-prefix wildcard-mask format to represent a group of addresses. This command was modified to support the UDA ACLs.</td>
</tr>
</tbody>
</table>
access-list (sequence)

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

Syntax

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

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

Parameters

**num**

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

**sequence number**

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

**permit**

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

**deny**

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

**vlan vlan-id**

Indicates the selected VLAN.

**protocol ipv6-source-prefix/prefix-length**

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

**ipv6-source-prefix wildcard-mask**

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

**any**

Specifies instead of the ipv6-source-prefix/prefix-length or ipv6-destination-prefix/prefix-length parameters it matches any IPv6 prefix and is equivalent to the IPv6 prefix ::/0.
The **host ipv6-source-address** and **host ipv6-destination-address** parameter lets you specify a host IPv6 address. When you use this parameter, you do not need to specify the prefix length. A prefix length of all 128 is implied.

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

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

**ipv6-destination-prefix wildcard-mask**

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

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

**host ipv6-destination-address**

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

**ipv6-operator value**

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

**copy-sflow**

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

**drop-precedence dp-value**

Sets the drop precedence by the selected value.

**drop-precedence-force dp-value**

Sets the force drop precedence by the selected value.

**dscp dscp-value**

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

**dscp-marking dscp-value**

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

**mirror**

Mirror packets matching the ACL permit clause.

**priorityforce number**

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

Global configuration mode.

Usage Guidelines

You can also create ACLs using the following commands:

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

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

Examples

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

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

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

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

```
device# configure terminal
device(config)# access-list 1 sequence 100 deny host 10.157.22.26
device(config)# access-list 1 sequence 200 deny 10.157.29.12
device(config)# access-list 1 sequence 300 deny host IPHost1
device(config)# access-list 1 sequence 400 permit any

device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group 1 in
```
The following example creates a numbered extended IPv4 ACL with an ID of 102, and defines sequential rules to:

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

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

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

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

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

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the <code>ipv6-source-prefix wildcard-mask</code> and <code>ipv6-destination-prefix wildcard-mask</code> format to represent a group of addresses.</td>
</tr>
</tbody>
</table>
activate (VRRP)

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

Syntax

```
activate
no activate
```

Command Default

A VRRP virtual routing instance is not activated.

Modes

- VRID interface configuration mode

Usage Guidelines

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

The no form of this command disables the VRRP VRID.

Examples

The following example configures and activates VRRP VRID 1.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
VRRP router 1 for this interface is activating
```
additional-paths
Enables additional paths capability for all BGP neighbors under the configured address family.

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

Command Default
Additional paths are not advertised.

Parameters
receive
   Enables BGP capability to receive additional paths from BGP neighbors.

send
   Enables BGP capability to send additional paths to BGP neighbors.

Modes
BGP address-family IPv4 unicast configuration mode
BGP address-family IPv6 unicast configuration mode
BGP address-family IPv4 multicast configuration mode
BGP address-family IPv6 multicast configuration mode
BGP address-family IPv4 unicast VRF configuration mode
BGP address-family IPv6 unicast VRF configuration mode

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

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

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

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

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
additional-paths select

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

Syntax

```
additional-paths select all [ best number ] [ group-best ]
additional-paths select best number [ all ] [ group-best ]
additional-paths select group-best [ all ] [ best number ]
no additional-paths select { all | best number | group-best }
```

Command Default

Paths are not selected.

Parameters

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

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

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

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

Modes

- BGP address-family IPv4 unicast configuration mode
- BGP address-family IPv6 unicast configuration mode
- BGP address-family IPv4 multicast configuration mode
- BGP address-family IPv6 multicast configuration mode
- BGP address-family IPv4 unicast VRF configuration mode
- BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The `no` form of the command removes the specified candidate from the filter list.
Examples

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

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

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

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

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
address-family multicast (BGP)

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

Syntax

address-family ipv4 multicast
address-family ipv6 multicast
no address-family ipv4 multicast
no address-family ipv6 multicast

Parameters

ipv4
  Specifies an IPv4 address family.
ipv6
  Specifies an IPv6 address family.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

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

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

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

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

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

Syntax

address-family ipv4 unicast [ vrf vrf-name ]
address-family ipv6 unicast [ vrf vrf-name ]
no address-family ipv4 unicast [ vrf vrf-name ]
no address-family ipv6 unicast [ vrf vrf-name ]

Parameters

ipv4
Specifies an IPv4 address family.

ipv6
Specifies an IPv6 address family.

vrf vrf-name
Specifies a VRF instance.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

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

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

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

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

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

Syntax

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

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

Parameters

num

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

use-threshold-table

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

Modes

MPLS auto-bandwidth template configuration mode.
MPLS LSP auto-bandwidth configuration mode.

Usage Guidelines

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

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

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

Examples

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

device(config)# router mpls
device(config-mpls)# autobw-template template1
device(config-mpls-autobw-template-template1)# adjustment-interval 1200
device(config-mpls-autobw-template-template1)# adjustment-threshold use-threshold-table
device(config-mpls-autobw-template-template1)# overflow-limit 10
device(config-mpls-autobw-template-template1)# underflow-limit 20
device(config-mpls-autobw-template-template1)# sample-recording enable
The following example under the MPLS lsp autobw config mode defines the automatic bandwidth adjustment threshold as 40 percent.

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

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
advertise backup

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

Syntax

advertise backup
no advertise backup

Command Default

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

Modes

VRID interface configuration mode

Usage Guidelines

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

The `advertise backup` command is configured only on VRRP backup routers and is supported by VRRP and VRRP-E. The `no` form of the command disables the advertisement of a VRRP backup router to a VRRP master router.

Examples

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

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

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

Syntax

advertise-best-external
no advertise-best-external

Command Default

The best external path is not calculated.

Modes

BGP address-family IPv4 unicast configuration mode
BGP address-family IPv6 unicast configuration mode
BGP address-family IPv4 multicast configuration mode
BGP address-family IPv6 multicast configuration mode
BGP address-family IPv4 unicast VRF configuration mode
BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The no form of the command disables the advertising of the best external route under the configured address family.

Examples

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**advertise-fec**

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

**Syntax**

```
advertise-fec prefix-list
no advertise-fec prefix-list
```

**Parameters**

`prefix-list`

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

**Modes**

MPLS LDP configuration mode.

**Usage Guidelines**

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

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

The no form of the command removes the prefix listing.

**Examples**

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

```
device(config)# ip prefix-list list-abc deny 44.44.44.44/32
device(config)# ip prefix-list list-abc permit 0.0.0.0/0 ge 32
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# advertise-fec list-abc
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
always-compare-med

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

Syntax

always-compare-med

no always-compare-med

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

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

Examples

This example configures the device always to compare the MEDs.

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

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

Syntax

area { ipv6-address | decimal } authentication ipsec spi value esp sha1 key [no-encrypt] key
no area { ipv6-address | decimal } authentication ipsec spi value

Command Default

Authentication is not enabled on an area.

The key is stored in encrypted format by default.

Parameters

ipv6-address

Specifies an IPv6 address.

decimal

Specifies an area address in decimal format.

ipsec

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

spi

Specifies the Security Policy Index (SPI).

value

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

esp

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

sha1

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

key

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

no-encrypt

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

key

The 40 hexadecimal character key.
Modes

OSPFv3 router configuration mode
OSPFv3 router VRF configuration mode

Usage Guidelines

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

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

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

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

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

Examples

The following example enables esp and SHA-1 authentication for an OSPFv3 area, setting a SPI value of 900.

```
device# configure terminal
device(config)# ip router-id 10.1.2.3
device(config)# ipv6 router ospf
device(config-ospf6-router)# area 0 authentication ipsec spi 750 esp sha1 abce12345678901234fedcba098765432109876
```
area nssa (OSPFv3)

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

Syntax

```plaintext
area { IPv6 address | decimal } nssa [ metric ] [ default-information-originate [ metric num ] [ metric-type { type-1 | type-2 } ] ]
[ no-redsitribution ] [ no-summary ] [ translator-always ] [ translator-interval interval]
```

no area nssa

Command Default

No areas are created.

Parameters

- **IPv6 address**
  Specifies an IPv6 address.

- **decimal**
  Area address in decimal format.

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

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

- **metric-type**
  Specifies how the cost of a neighbor metric is determined.

  - **type-1**
    The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.

  - **type-2**
    The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

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

- **no-summary**
  When configured on the NSSA area border router (ABR), this parameter prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA a NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs. **Note:** This parameter is disabled by default, which means the default route must use a Type 7 LSA.
**translator-always**

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

**translator-interval interval**

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

### Modes

- OSPFv3 router configuration mode
- OSPFv3 router VRF configuration mode

### Usage Guidelines

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

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

The no form of the command deletes a NSSA.

### Examples

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

```
device# configure terminal
device(config)#ipv6 router ospf
device(config-ospf6-router)# area 8 nssa 4 no-summary
```
area range (OSPFv2)

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

Syntax

```
area { A.B.C.D | decimal } range E.F.G.H I.J.K.L [ advertise | not-advertise ] [ cost cost_value ]
no area range
```

Command Default

The address range is advertised.

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format.

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

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

advertise

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

cost cost_value

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

not-advertise

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

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

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

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

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

**Examples**

The following example advertises to Area 3 all the addresses on the network 10.1.1.0 10.255.255.0 in the ABR you are signed into.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# area 3 range 10.1.1.0 10.255.255.0 advertise
```
area range (OSPFv3)

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

Syntax

```
area { IPv6 address | decimal } range ipv6 address/mask [ advertise | not-advertise ] [ cost cost_value ]
no area range
```

Parameters

- IPv6 address
  - Specifies an IPv6 address.
- decimal
  - Area address in decimal format.
- ipv6 address/mask
  - Specifies the IPv6 address in dotted-decimal notation and the IPv6 mask in CIDR notation. All network addresses that match this network are summarized in a single route and advertised by the ABR.
- advertise
  - Sets the address range status to advertise and generates a Type 3 summary LSA.
- cost cost_value
  - Sets the cost value for the area range. This value is used as the generated summary LSA cost. The range for cost_value is 1 to 6777214. If this value is not specified, the cost value is the default range metric calculation for the generated summary LSA cost.
- not-advertise
  - Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting is used to temporarily pause route summarization from the area.

Modes

- OSPFV3 router configuration mode
- OSPFV3 router VRF configuration mode

Usage Guidelines

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

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

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

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

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

Creates or deletes a stub area or modifies its parameters.

Syntax

```
area { A.B.C.D | decimal } stub metric [ no-summary ]
no area stub
```

Command Default

No areas are created.

Parameters

- **A.B.C.D**
  Area address in dotted decimal format.

- **decimal**
  Area address in decimal format.

- **metric**
  Additional cost for using a route to or from this area. Valid values range from 3 through 1048575 in OSPFv3 router and OSPFv3 router VRF configuration mode. Valid values range from 1 through 677215 in OSPF router and OSPF router VRF configuration mode.

- **no-summary**
  When configured on the ABR, this parameter prevents any Type 3 and Type 4 summary LSAs from being injected into the area. The only exception is that a Type 3 LSA. Enabling this parameter makes the area a so-called totally stubby area, which can only have Types 1 and 2. This parameter is disabled by default.

Modes

- OSPF router configuration mode
- OSPF router VRF configuration mode
- OSPFv3 router configuration mode
- OSPFv3 router VRF configuration mode

Usage Guidelines

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

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

The following example sets an additional cost of 5 on a stub area called 2 (in decimal format).

```plaintext
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# area 2 stub 5
```
area virtual-link (OSPFv3)

Creates or modifies virtual links for an area.

Syntax

```plaintext
area IPv6 address | decimal virtual-link A.B.C.D [ dead-interval time | hello-interval time | hello-jitter interval | retransmit-interval time | transmit-delay time ]
no area virtual-link
```

Command Default

No virtual links are created.

Parameters

- **IPv6 address**
  Specifies an IPv6 address.

- **decimal**
  Area address in decimal format.

- **A.B.C.D**
  ID of the OSPFv3 device at the remote end of the virtual link.

- **dead-interval time**
  How long a neighbor device waits for a hello packet from the current device before declaring the device down. This value must be the same for all devices and access servers that are attached to a common network. Valid values range from 1 through 65535 seconds. The default is 40 seconds.

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

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

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

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

- OSPFv3 router configuration mode
- OSPFv3 router VRF configuration mode

Usage Guidelines

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

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

Examples

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

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# area 1 virtual-link 209.157.22.1
```
area virtual-link authentication (OSPFv3)

Enables authentication for virtual links in an OSPFv3 area.

Syntax

```
area { IPv6 address | decimal } virtual-link E.F.G.H authentication ipsec spi value esp sha1 key [ no-encrypt ] key
no area { IPv6 address | decimal } virtual-link E.F.G.H authentication ipsec spi spi
```

Command Default

Authentication is not enabled on a virtual-link.

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

Parameters

- **IPv6 address**: Specifies an IPv6 address.
- **decimal**: Area address in decimal format.
- **E.F.G.H**: ID of the OSPFv3 device at the remote end of the virtual link.
- **ipsec**: Specifies that IP security (IPsec) is the protocol that authenticates the packets.
- **spi**: Specifies the Security Policy Index (SPI).
- **value**: Specifies the SPI value. Valid values range from decimal numbers 256 through 4294967295. The near-end and far-end values must be the same.
- **esp**: Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security. This is the only option currently available.
- **sha1**: Enables Hashed Message Authentication Code (HMAC) Secure Hash Algorithm 1 (SHA-1) authentication on the OSPFv3 area.
- **key**: Number used in the calculation of the message digest. The 40 hexadecimal character key is stored in encrypted format by default.
- **no-encrypt**: The 40-character key is not encrypted upon either its entry or its display.
The 40 hexadecimal character key.

**Modes**

- OSPFv3 router configuration mode
- OSPFv3 router VRF configuration mode

**Usage Guidelines**

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

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

**Examples**

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

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

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

Syntax

arp ip_addr mac_addr [ ethernet slot/port | vlan vlan_id ]
no arp ip_addr mac_addr [ ethernet slot/port | vlan vlan_id ]
arp ip_addr mac_addr [ multi-ports { ethernet slot/port [ ethernet slot/port . . . ] | ethernet slot/port to slot/port } | { pos slot/port [ pos slot/port . . . ] | pos slot/port to slot/port } ]
no arp ip_addr mac_addr [ multi-ports { ethernet slot/port [ ethernet slot/port . . . ] | ethernet slot/port to slot/port } | { pos slot/port [ pos slot/port . . . ] | pos slot/port to slot/port } ]
arp ip_addr mac_addr [ multi-ports { ethernet slot/port ethernet slot/port ethernet slot/port | ethernet slot/port to slot/port } | { pos slot/port pos slot/port pos slot/port | slot/port to slot/port } ]
no arp ip_addr mac_addr [ multi-ports { ethernet slot/port ethernet slot/port ethernet slot/port | ethernet slot/port to slot/port } | { pos slot/port pos slot/port pos slot/port | slot/port to slot/port } ]
arp ip_addr mac_addr [ vpls { peer ip_addr | vlan vlan_id ethernet slot/port } ]
no arp ip_addr mac_addr [ vpls { peer ip_addr | vlan vlan_id ethernet slot/port } ]

Parameters

ip_addr
   Specifies the IPv4 address of the host.

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

ethernet slot/port
   Specifies the selected Ethernet port.

multi-ports
   Configures multi-ports static ARP. See “Usage Guidelines.”

   ethernet
      Configures the static ARP entry on the Ethernet port.

   pos
      Configures the static ARP entry on the POS port.

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

vpls
   Configures static ARP entry for a VPLS instance.

peer
   Configures the VPLS-peer IP address.
**vlan**

Configures the VLAN ID.

**Modes**

- Global configuration mode.
- VRF sub-configuration mode.

**Usage Guidelines**

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

- If the VLAN ID is not configured when IP source guard is turned on, the IP address is assumed to be valid on all the VLANS on the port.
- If both the VLAN ID and the port are not configured when IP source guard is turned on, the IP address is assumed to be valid for all VLANS.
- The multi-ports option allows you to assign multiple ports in the same VE to a single static ARP entry. The option can be used in a pure Layer 3 forwarding environment to forward IPv4 traffic from multiple ports but should not be used in conjunction with multiport static MAC. When you use the multi-ports option, you can create a list of interfaces, a range of interfaces, or a combination. You can use multiple lists and ranges in the same command line.

**Examples**

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

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

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

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

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

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

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was modified to enable VRF for VPLS VE.</td>
</tr>
</tbody>
</table>
arp-guard
Discards all gratuitous ARP and ARP replies for IP addresses not permitted by the specified ARP-guard standard IP access control list (ACL).

Syntax
arp-guard arp-guard-access-list-name
no arp-guard arp-guard-access-list-name

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

Parameters
arp-guard-access-list-name
ARP packets that do not match the specified ARP guard ACL are dropped by the LP and those which match will be software forwarded.

Modes
Interface configuration mode

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

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

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
arp-guard-access-list

Creates the ARP guard access list.

Syntax

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

Command Default

No ARP guard access list is created.

Parameters

 arp-guard-access-list-name

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

Modes

Global configuration mode.

Usage Guidelines

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

Examples

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
**arp-guard-syslog-timer**

Sets the system log timer duration for an ARP guard.

**Syntax**

```
arp-guard-syslog-timer dec
no arp-guard-syslog-timer dec
```

**Command Default**

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

**Parameters**

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

**Modes**

Global configuration mode.

**Usage Guidelines**

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

**Examples**

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

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

```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
as-path-ignore

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

Syntax

- `as-path-ignore`
- `no as-path-ignore`

Command Default

This feature is disabled.

Modes

- BGP configuration mode

Usage Guidelines

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

Examples

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

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# as-path-ignore
```
authentication (IKEv2)

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

Syntax

```
authentication authentication-proposal-name
```

Parameters

`authentication-proposal-name`

Specifies the name of an authentication proposal.

Modes

IKEv2 profile configuration mode

Examples

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
auto-bandwidth

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

Syntax

auto-bandwidth sample-interval sec

no auto-bandwidth sample-interval sec

Parameters

sample-interval sec

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

Modes

Global configuration mode.

MPLS configuration mode (config-mpls-policy).

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**autobw-threshold-table**

Configures the MPLS auto-bandwidth threshold table.

**Syntax**

```
autobw-threshold-table

no autobw-threshold table
```

**Modes**

- MPLS configuration mode.
- MPLS auto-bandwidth threshold table configuration mode.
- MPLS LSP configuration mode.

**Usage Guidelines**

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

**Examples**

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

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

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

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

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

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

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

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

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
auto-cost reference-bandwidth (OSPFv2)

Configures reference bandwidth.

Syntax

```plaintext
auto-cost reference-bandwidth { value | use-active-ports }
no auto-cost reference-bandwidth
```

Command Default

Reference bandwidth is 100 Mbps.

Parameters

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

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

Modes

- OSPF router configuration mode
- OSPF router VRF configuration mode

Usage Guidelines

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

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

- **LAG group** — The combined bandwidth of all the ports.
- **Virtual interface** — The combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

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

**NOTE**

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

The `no` form of the command disables bandwidth configuration.
Examples

The following example configures a reference bandwidth of 500.

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

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

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

The costs for 10 Mbps and 100 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.
auto-cost reference-bandwidth (OSPFv3)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth value
no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

value

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

Modes

OSPFv3 router configuration mode
OSPFv3 router VRF configuration mode

Usage Guidelines

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

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

- LAG group — The combined bandwidth of all the ports.
- Virtual (Ethernet) interface — The combined bandwidth of all the ports in the port-based VLAN that contains the virtual interface.

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

**NOTE**

If you specify the cost for an individual interface using the `ipv6 ospf cost` command, the cost you specify overrides the cost calculated by the software.

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

- The cost of a loopback interface is always 1.
- The cost of a virtual link is calculated using the Shortest Path First (SPF) algorithm and is not affected by the auto-cost feature.
- The bandwidth for tunnel interfaces is 9 Kbps and is subject to the auto-cost feature.
Enter no form of the command restores the reference bandwidth to its default value and, thus, restores the default costs of the interfaces to their default values.

Examples

The following example configures a reference bandwidth of 500.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# auto-cost reference-bandwidth 500
```

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

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

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

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

Syntax

auto-enroll [ regenerate | percent ]

no auto-enroll [ regenerate | percent ]

Command Default

The option to send enrollment messages is disabled.

Parameters

regenerate

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

percent

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

Modes

PKI trustpoint configuration mode.

Usage Guidelines

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

Examples

The following example specifies the percentage value as 20.

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

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**auto-shutdown-new-neighbors**
Disables the establishment of BGP connections with a remote peer when the peer is first configured.

**Syntax**
```
auto-shutdown-new-neighbors
no auto-shutdown-new-neighbors
```

**Command Default**
This feature is disabled.

**Modes**
BGP configuration mode

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

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

**Examples**
The following example enables auto shutdown of BGP neighbors on initial configuration.
```
device# configure terminal
device(config)# router bgp
device(config-bgp)# auto-shutdown-new-neighbors
```
backup

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

Syntax

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

Command Default

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

Parameters

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

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

Modes

VRID interface configuration mode

Usage Guidelines

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

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

This command must be entered before the ip-address command can be configured for a VRRP or VRRP-E virtual routing ID. The no form of this command removes the virtual router configuration.
Examples

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

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

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

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

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

Syntax

backup-bw-best-effort

no backup-bw-best-effort

Command Default

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

Modes

MPLS RSVP configuration mode.

Usage Guidelines

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

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

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

Examples

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
backup-hello-interval

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

Syntax

```
backup-hello-interval seconds
no backup-hello-interval seconds
```

Command Default

The default backup hello interval is 60 seconds.

Parameters

```
seconds
```

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

Modes

VRID interface configuration mode

Usage Guidelines

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

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

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

Examples

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

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

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

**Syntax**

```
bandwidth { inherit | dec }
no bandwidth { inherit | dec }
```

**Command Default**

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

**Parameters**

- **inherit**
  - **dec**

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

**Modes**

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

**Usage Guidelines**

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

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

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

**Examples**

Display output of the `bandwidth` command:

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

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
bandwidth-ceiling

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

Syntax

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

Parameters

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

- **max**
  
  Defines the threshold for any traffic-rate as infinity.

- **threshold** **threshold_in_kbps**
  
  Sets the threshold to be used up to this defined ceiling.

Modes

- MPLS auto-bandwidth threshold table configuration mode.

Usage Guidelines

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

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

Examples

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

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

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

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

The following example shows how to clear the threshold table.

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
bandwidth-ceiling max threshold percentage

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

Syntax

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

Parameters

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

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

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

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

Modes

MPLS auto-bandwidth threshold table configuration mode.

Usage Guidelines

The no function of this command removes the entry.

Examples

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

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

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05:6.00</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
**base vrf**

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

**Syntax**

```text
base vrf base-vrf-name
no base vrf base-vrf-name
```

**Command Default**

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

**Parameters**

- `base-vrf-name`
  
  Specifies the VRF name of the base network.

**Modes**

Tunnel interface configuration mode

**Usage Guidelines**

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

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

**Examples**

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

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

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**bfd**
Configures Bidirectional Forwarding Detection (BFD) session parameters on BGP-enabled interfaces.

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

**Command Default**
Default parameters are used.

**Parameters**
- **min-tx transmit-time**
  Specifies the interval, in milliseconds, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000. The default is 1000 unless changed using the `bfd interval` command in interface sub-type configuration mode.

- **min-rx receive-time**
  Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000. The default is 1000 unless changed using the `bfd interval` command in interface sub-type configuration mode.

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

**Modes**
- BGP configuration mode
- BGP address-family IPv4 unicast VRF configuration mode

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

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

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

- The `min-tx`, `min-rx`, and `multiplier` keywords can also be configured for each peer and peer group and will override the global configuration.
When Brocade NetIron CER Series or Brocade NetIron CES Series devices are heavily loaded or under stress, BFD sessions may flap if the configured BFD interval is less than 500 milliseconds with a multiplier value of 3.

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

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

Examples

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

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

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

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

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

**Syntax**

```
bfd all-interfaces all-vrfs
bfd all-interfaces
no bfd all-interfaces all-vrfs
no bfd all-interfaces
```

**Command Default**

BFD is disabled by default.

**Parameters**

```
all-vrfs
```

Specifies all VRFs.

**Modes**

- IS-IS router configuration mode
- OSPF router configuration mode
- OSPFv3 router configuration mode
- OSPF router VRF configuration mode

**Usage Guidelines**

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

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

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

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

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

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

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

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

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

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

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

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

device# configure terminal
device(config)# router isis
device(config-isis-router)# bfd all-interfaces
**bfd holdover-interval**

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

**Syntax**

```
bfd holdover-interval time
no bfd holdover-interval time
```

**Command Default**

The BFD holdover interval is set to 0 by default.

**Parameters**

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

**Modes**

- BGP configuration mode
- BGP address-family IPv4 unicast VRF configuration mode
- IS-IS router configuration mode
- OSPF router configuration mode
- OSPFv3 router configuration mode
- OSPF router VRF configuration mode

**Usage Guidelines**

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

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

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

The `no` form of the command removes the configured BFD holdover interval from the configuration, and reverts to the default value of 0.
Examples

The following example sets the BFD holdover interval globally to 15 in BGP configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# bfd holdover-interval 15
```

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

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf-red)# bfd holdover-interval 15
```

The following example sets the BFD holdover interval globally to 12 in OSPF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# bfd holdover-interval 12
```

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

```
device# configure terminal
device(config)# router ospf vrf red
device(config-ospf-router-vrf-red)# bfd holdover-interval 12
```

The following example sets the BFD holdover interval globally to 20 in OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# bfd holdover-interval 20
```

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

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

Configures Bidirectional Forwarding Detection (BFD) session parameters on an interface.

Syntax

```
bfdf interval transmit-time min-rx receive-time multiplier number
no bfd interval transmit-time min-rx receive-time multiplier number
```

Command Default

Default parameters are used.

Parameters

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

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

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

Modes

```
Interface subtype configuration mode
```

Usage Guidelines

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

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

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

Examples

The following example sets the BFD session parameters globally for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# bfd interval 100 min-rx 100 multiplier 4
```
**bfd-enable**

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

**Syntax**

```
bfd-enable
no bfd-enable
```

**Command Default**

BFD is disabled by default.

**Modes**

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

**Usage Guidelines**

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

This command overrides all other BGP BFD configurations.

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

**Examples**

The following example enables BFD globally for BGP.

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

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

```
device# configure terminal
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# bfd-enable
```
**bfd mh-session-setup-delay**

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

**Syntax**

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

**Command Default**

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

**Parameters**

`seconds`

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

**Modes**

Global configuration mode

**Usage Guidelines**

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

**Examples**

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

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

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**bfd sh-session-setup-delay**

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

**Syntax**

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

**Command Default**

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

**Parameters**

*seconds*

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

**Modes**

Global configuration mode

**Usage Guidelines**

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

**Examples**

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

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

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
cam ifsr

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

Syntax

```
cam ifsr { disable | enable }
```

Command Default

Parameters

- **disable**
  
  Disables IFSR for TCAM hardware errors for a specified host name.

- **enable**
  
  Enables IFSR for TCAM hardware errors for a specified host name.

Modes

- Global configuration mode

Usage Guidelines

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

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

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

Examples

The following example enables IFSR.

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

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
cam-mode amod

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

Syntax

```
cam-mode amod slot number
no cam-mode amod slot number
```

Command Default

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

Parameters

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

- **number**
  
  Specifies the slot number.

Modes

Global configuration mode

Usage Guidelines

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

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

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

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

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

**NOTE**

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

Examples

The following example configures Algorithmic mode on slot 2.

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

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
capability as4

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

Syntax

capability as4-enable { disable | enable }

no capability

Command Default

This feature is disabled.

Parameters

disable

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

enable

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

Modes

BGP configuration mode

Usage Guidelines

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

Examples

The following example enables 4-byte ASN capability.

device# configure terminal
device(config)# router bgp
device(config-bgp)# capability as4-enable
clear access-list receive accounting

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

**Syntax**

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

**Parameters**

- **all**
  Specifies clearing accounting statistics for all configured IPv4 rACLs.

- **name acl-name**
  Clears accounting statistics for the specified IPv4 rACL.

**Modes**

Privileged EXEC mode.

**Usage Guidelines**

This command is also available in global configuration mode.

**Examples**

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

```
device(config)# clear access-list receive accounting name acl_ext1
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear arp-guard-statistics

Clears the different statistical information of the ARP guard.

Syntax

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

Command Default

Clears all statistics related to the ARP guard.

Parameters

all

Clears all ARP guard statistics.

ethernet slot/port

Specifies the defined Ethernet port to clear.

vlan vlan_id

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

Modes

EXEC mode.

Usage Guidelines

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

Examples

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

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan-id</th>
<th>Total_Arp_pkts_captured</th>
<th>Total_Arp_pkts_forwarded</th>
<th>Total_Arp_pkts_dropped</th>
<th>LAG : Prim</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1 (Def/Untag)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2/1 (Def/Untag)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2/1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2/1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2/1</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
The following example indicates clearing statistics information for any individual ports.

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

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

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

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

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

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear bm histogram

Clears buffer histogram data.

Syntax

clear bm histogram

Modes

Privileged EXEC mode

Usage Guidelines

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

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

Examples

The following example clears buffer histogram data.

device# clear bm histogram

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear cpu histogram sequence

Clears CPU histogram sequential execution of task data.

Syntax

```
clear cpu histogram sequence
no clear cpu histogram sequence
```

Modes

- Privileged EXEC mode.
- Global configuration mode.

Usage Guidelines

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

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

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

Examples

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

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

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear dot1x-mka statistics

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

Syntax

clear dot1x-mka statistics ethernet slot/port

Parameters

ethernet slot port

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

Modes

Privileged EXEC mode

Examples

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

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

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear ikev2 statistics

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

Syntax

clear ikev2 statistics

Modes

Privileged EXEC mode

Examples

The following example clears IKEv2 statistics from the device.

device# clear ikev2 statistics

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to add support for IPsec IPv6.</td>
</tr>
</tbody>
</table>
clear ikev2 sa
Clears Internet Key Exchange version 2 security associations (IKEv2 SAs).

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

Parameters
- `fvrf vrf-name`
  Specifies the front-door VRF (FVRF) for the SAs.
- `ipv4`
  Specifies clearing IPv4 connections.
- `ipv6`
  Specifies clearing IPv6 connections.
- `local ip-address`
  Specifies the IP address for the local interface. Both IPv4 and IPv6 address formats are supported.
- `remote ip-address`
  Specifies the IP address for the remote interface. Both IPv4 and IPv6 address formats are supported.

Modes
Privileged EXEC mode

Usage Guidelines
The clearing process deletes and re-establishes the SAs (including any child SAs).
When optional parameters are not specified, the command clears all IKEv2 SAs on the device.

Examples
The following example clears the IKEv2 SAs for local interface 10.10.20.1.
```
device# clear ikev2 sa local 10.10.20.1
```

The following example clears the IKE SAs for remote interface 10.0.10.1.
```
device# clear ikev2 sa remote 10.0.10.1
```

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to add support for IKEv2 IPv6.</td>
</tr>
</tbody>
</table>
clear ip bgp dampening
    Reactivates suppressed BGP4 routes.

Syntax
    clear ip bgp dampening \[ ip-addr \[ / mask \] \]

Parameters
    ip-addr
        IPv4 address of a specified route in dotted-decimal notation.
    mask
        IPv4 mask of a specified route in CIDR notation.

Modes
    Privileged EXEC mode

Examples
    The following example unsuppresses all suppressed BGP4 routes.
    device# clear ip bgp dampening
**clear ip bgp flap-statistics**

Clears the dampening statistics for a BGP4 route without changing the dampening status of the route.

**Syntax**

```
clear ip bgp flap-statistics [ ip-addr | mask | neighbor ip-addr | regular-expression string ]
```

**Parameters**

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

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

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

  - `ip-addr`
    IPv4 address of the neighbor.

- `regular-expression`
  Specifies a regular expression.

  - `string`
    Regular expression.

**Modes**

Privileged EXEC mode

**Examples**

This example clears the dampening statistics for a BGP4 route.

```
device# clear ip bgp flap-statistics 10.0.0.0/16
```
clear ip bgp local routes
Clears BGP4 local routes from the IP route table and resets the routes.

Syntax
  clear ip bgp local routes

Modes
  Privileged EXEC mode

Examples
  This example clears all BGP4 local routes.
  
  device# clear ip bgp local routes
clear ip bgp neighbor
Requests a dynamic refresh of BGP4 connections or routes from a neighbor, with a variety of options.

Syntax
```
clear ip bgp neighbor { all | as-num | peer-group-name | ip-addr } [ last-packet-with-error ] [ notification-errors ] [ soft [ in | out ] ] [ soft-outbound ] [ traffic ]
```

Parameters
- **all**
  Resets and clears all BGP4 connections to all neighbors.
- **as-num**
  Clears all BGP4 connections within this autonomous system. Range is from 1 through 4294967295.
- **peer-group-name**
  Clears all BGP4 connections in this peer group. Range is from 1 through 63 characters.
- **ip-addr**
  Clears all BGP4 connections with this IPv4 address, in dotted-decimal notation.
- **last-packet-with-error**
  Clears all BGP4 connections identified as having the last packet received with an error.
- **notification-errors**
  Clears all BGP4 connections identified as having notification errors.
- **soft**
  Refreshes routes received from or sent to the neighbor.
  - **in**
    Refreshes received routes.
  - **out**
    Refreshes sent routes.
- **soft-outbound**
  Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

  **NOTE**
  Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4 route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.
- **traffic**
  Clears the counters (resets them to 0) for BGP4 messages.
Modes

Privileged EXEC mode

Examples

The following example refreshes all BGP4 neighbor connections.

device# clear ip bgp neighbor all
clear ip bgp routes
  Clears BGP4 routes from the IP route table and resets the routes.

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

Parameters
  ip-addr
    IPv4 address of a specified route in dotted-decimal notation.
  mask
    (Optional) IPv4 mask of a specified route in CIDR notation.

Modes
  Privileged EXEC mode

Examples
  This example clears all BGP4 routes.

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

Clears the BGP4 message counter for all neighbors.

Syntax

clear ip bgp traffic

Modes

Privileged EXEC mode

Examples

The following example clears the BGP4 message counters:

device# clear ip bgp traffic
**clear ip bgp vrf**
Cleans BGP4 information for a virtual routing and forwarding (VRF) instance.

**Syntax**
```
clear ip bgp vrf vrf-name
```

**Parameters**
- **vrf vrf-name**
  Specifies the name of a VRF instance.

**Modes**
Privileged EXEC mode

**Examples**
The following example clears BGP4 information for VRF red.
```
device# clear ip bgp vrf red
```
clear ip vrrp statistics


Syntax

clear ip vrrp statistics

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring VRRP options, for example, and want to clear existing statistics.

Examples

The following example clears IPv4 VRRP statistics when entered in privileged EXEC mode.

device# clear ip vrrp statistics

The following example clears IPv4 VRRP statistics when entered in VRID interface configuration mode.

device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# clear ip vrrp statistics
clear ip vrrp-extended statistics


Syntax

```
clear ip vrrp-extended statistics
```

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring VRRP-E options, for example, and want to clear existing statistics.

Examples

The following example clears IPv4 VRRP-E statistics when entered in privileged EXEC mode.

```
device# clear ip vrrp-extended statistics
```

The following example clears IPv4 VRRP-E statistics when entered in VRID interface configuration mode.

```
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.1/24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# clear ip vrrp-extended statistics
```
clear ipsec error-count
Clears the error counters for the IPsec errors.

Syntax
\[\text{clear ipsec error-count}\]

Modes
Privileged EXEC mode.

Examples
The following example clears the error counters for the IPsec errors.
\[\text{device\# clear ipsec error-count}\]

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Commands A - E
clear ipsec sa

Clears IPsec security associations (SAs).

Syntax

clear ipsec sa [ fvrf vrf-name | ipv4 | ipv6 | peer ip-address ]

Parameters

fvrf vrf-name

Specifies the front-door VRF (FVRF) for the SAs.

ipv4

Specifies clearing IPv4 associations.

ipv6

Specifies clearing IPv6 associations.

peer ip-address

Specifies the IP address for the peer interface. Both IPv4 and IPv6 address formats are supported.

Modes

Privileged EXEC mode

Usage Guidelines

The clearing process deletes and re-establishes IPsec SAs. The SAs remain unchanged.

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

Examples

The following example clears all IPsec SAs on the device.

device# clear ipsec sa

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to add support for IPsec IPv6.</td>
</tr>
</tbody>
</table>
clear ipsec statistics

Clears IPsec system counters (such as ESP packet counts and IPsec error counts), and IPsec tunnel packet and byte counts (such as transmitted and received packets).

Syntax

```
clear ipsec statistics [ all ]
```

Parameters

`all`

(Optional) Specifies that all IPsec statistics should be cleared (this includes system counters and IPsec tunnel packet counts and byte counts).

Modes

Privileged EXEC mode.

Usage Guidelines

This command supports IPsec IPv4 and IPv6.

When you omit the optional `all` parameter, only the system counters (such as ESP packet counts and IPsec error counts) are cleared. When you include the `all` parameter, the system counters and IPsec tunnel packet and byte counts are also cleared.

Examples

The following example clears the IPSec system counters.

```
device# clear ipsec statistics
```

The following example clears all of the IPsec statistics, including system counters and IPsec tunnel packet and byte counts.

```
device# clear ipsec statistics all
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was modified to add the <code>all</code> keyword.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to add support for IPsec IPv6.</td>
</tr>
</tbody>
</table>
clear ipsec statistics tunnel
Clears the IPsec tunnel packet and bytes counters.

Syntax
```
clear ipsec statistics tunnel dec | all
```

Parameters
- **dec**
  - Clears the IPsec counter for the tunnel specified by its ID number.
- **all**
  - Clears the IPsec counters for all tunnels.

Modes
- User EXEC mode.
- Privileged EXEC mode.

Examples
The following example clears the IPsec tunnel packet and bytes counters.
```
device# clear ipsec statistics tunnel
```

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear ipv6 bgp dampening
Reactivates suppressed BGP4+ routes.

Syntax

```
clear ipv6 bgp dampening [ ipv6-addr { / mask } ]
```

Parameters

- `ipv6-addr`
  IPv6 address of a specified route in dotted-decimal notation.

- `mask`
  IPv6 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

The following example unsuppresses all suppressed BGP4+ routes.

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

Clears the dampening statistics for a BGP4+ route without changing the dampening status of the route.

Syntax

```
clear ipv6 bgp flap-statistics [ ipv6-addr / mask | neighbor ipv6-addr | regular-expression string ]
```

Parameters

- `ipv6-addr`
  - IPv6 address of a specified route in dotted-decimal notation.
- `mask`
  - (Optional) IPv6 mask of a specified route in CIDR notation.
- `neighbor`
  - Clears dampening statistics only for routes learned from the specified neighbor.
  - `ipv6-addr`
    - IPv6 address of the neighbor.
- `regular-expression`
  - Specifies a regular expression.
  - `string`
    - Regular expression.

Modes

- Privileged EXEC mode

Examples

This example clears the dampening statistics for a BGP4+ route.

```
device# clear ip bgp flap-statistics 2001:2002::23:61
```
clear ipv6 bgp local routes
Clears BGP4+ local routes from the IP route table and resets the routes.

Syntax

   clear ipv6 bgp local routes

Modes

   Privileged EXEC mode

Examples

   This example clears all BGP4+ local routes.

   device# clear ipv6 bgp local routes
**clear ipv6 bgp neighbor**

Requests a dynamic refresh of BGP4+ connections or routes from a neighbor, with a variety of options.

**Syntax**

```plaintext
clear ipv6 bgp neighbor { all | as-num | peer-group-name | ipv6-addr } [ last-packet-with-error ] [ notification-errors ] [ soft [ in | out ] ] [ soft-outbound ] [ traffic ]
```

**Parameters**

- **all**
  - Resets and clears all BGP4+ connections to all neighbors.

- **as-num**
  - Clears all BGP4+ connections within this autonomous system. Range is from 1 through 4294967295.

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

- **ipv6-addr**
  - Clears all BGP4+ connections with this IPv6 address, in dotted-decimal notation.

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

- **notification-errors**
  - Clears all BGP4+ connections identified as having notification errors.

- **soft**
  - Refreshes routes received from or sent to the neighbor.

  - **in**
    - Refreshes received routes.

  - **out**
    - Refreshes sent routes.

- **soft-outbound**
  - Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

  **NOTE**
  
  Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4+ route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

- **traffic**
  - Clears the counters (resets them to 0) for BGP4+ messages.
Modes

Privileged EXEC mode

Examples

The following example refreshes all BGP4+ neighbor connections.

device# clear ipv6 bgp neighbor all
clear ipv6 bgp routes

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

Syntax

```
    clear ipv6 bgp routes [ ipv6-addr { / mask } ]
```

Parameters

- **ipv6-addr**
  IPv6 address of a specified route in dotted-decimal notation.

- **mask**
  (Optional) IPv6 mask of a specified route in CIDR notation.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4+ routes.

```
device# clear ipv6 bgp routes
```
clear ipv6 bgp traffic
   Clears the BGP4+ message counter for all neighbors.

Syntax
   clear ipv6 bgp traffic

Modes
   Privileged EXEC mode

Examples
   The following example clears the BGP4+ message counters.

   device# clear ipv6 bgp traffic
clear ipv6 vrrp statistics


Syntax

```
clear ipv6 vrrp statistics
```

Modes

- Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring IPv6 VRRP options, for example, and want to clear existing VRRP statistics.

Examples

The following example clears IPv6 VRRP statistics when entered in privileged EXEC mode.

```
device# clear ipv6 vrrp statistics
```

The following example clears IPv6 VRRP statistics when entered in VRID interface configuration mode.

```
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ipv6 vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# clear ipv6 vrrp statistics
```
clear ipv6 vrrp-extended statistics


Syntax

clear ipv6 vrrp-extended statistics

Modes

Privileged EXEC mode

Usage Guidelines

This command can be entered in privileged EXEC mode and in any configuration mode. Entering the command in a configuration mode can be useful if you are configuring IPv6 VRRP-E options, for example, and want to clear existing VRRP-E statistics.

Examples

The following example clears IPv6 VRRP-E statistics when entered in privileged EXEC mode.

device# clear ipv6 vrrp-extended statistics

The following example clears IPv6 VRRP-E statistics when entered in VRID interface configuration mode.

device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 2001:DB8::2/24
device(config-if-e1000-1/5)# ipv6 vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# clear ipv6 vrrp-extended statistics
clear isis shortcut

Clears IS-IS shortcuts on LSPs. IS-IS attempts to re-map the LSP To address to the IS-IS system ID.

Syntax

```
clear isis shortcut [ lsp lsp-name | registration ]
```

Parameters

- `lsp lsp-name`
  
  Clears the IS-IS shortcuts from the specified LSP.

- `registration`
  
  Reregisters IS-IS with MPLS.

Modes

Privileged EXEC mode.

Usage Guidelines

**NOTE**

The clearing of IS-IS shortcuts is not a common operation.

Clearing shortcuts is useful when the mapping between the To address and System ID must be refreshed after the LSP tunnel is being used in the SPF calculation.

If you do not specify an LSP, the command clears all IS-IS shortcuts from the configuration.

Examples

The following example shows the clearing of IS-IS shortcuts for the tunnel3 LSP.

```
device# clear isis shortcut lsp tunnel3
```
clear macsec statistics
Clears the MACsec traffic statistics for the specified interface.

Syntax
```
clear macsec statistics ethernet slot/port
```

Parameters
- `ethernet slot/port`
  Specifies an Ethernet interface by slot on the device, and interface on the slot.

Modes
- Privileged EXEC mode.

Usage Guidelines
This command operates in all modes.

Examples
In the following example, MACsec traffic statistics are cleared for interface 3/2.
```
device(config)# clear macsec statistics ethernet 3/2
MACsec statistics cleared
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear memory histogram

Clears memory histogram data.

Syntax

```
clear memory histogram
```

Modes

Privileged EXEC mode.

Usage Guidelines

This command operates in all modes.

The memory histogram keeps track of each memory allocation/deallocation request from an application. It helps to identify memory leak and memory usage across the task. It also monitors the under usage condition and reports to the system. The memory histogram is recorded when available memory goes below the threshold limit on each memory pool.

Before starting another collection cycle, it may be useful to clear the existing memory histogram information using the `clear memory histogram sequence` command. This command can also be entered in global configuration mode.

To view the memory histogram information, use the `show memory histogram` command.

Examples

The following example clears memory histogram data.

```
device(config)# clear memory histogram
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>
clear metro mp-vlp-queue

Resets the management processor virtual line card (MP-VLP) queue statistics on Brocade NetIron CER Series devices.

Syntax

clear metro mp-vlp-queue

Modes

Privileged EXEC mode.

Usage Guidelines

this command operates in all modes.

show metro mp-vlp-queue

Examples

This example clears all the counters in the MP-VLP queue statistics.

device# clear metro mp-vlp-queue

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear mpls auto-bandwidth-samples

Deletes the sample-history from the auto-bandwidth LSPs.

Syntax

clear mpls auto-bandwidth-samples [ all | lsp lsp_name ]

Parameters

all

Clear all of the auto-bandwidth sample history.

lsp lsp_name

Clears the auto-bandwidth sample history for the specified LSP.

Modes

Privileged EXEC mode.

Usage Guidelines

Samples are not deleted or deallocated when the LSP is disabled or when auto-bandwidth is disabled at the global or LSP level.

Examples

The following example shows the command used to clear all of the auto-bandwidth sample history.

device# clear mpls auto-bandwidth-samples all

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear mpls ldp neighbor

Resets all LDP sessions on the Brocade device or the LDP sessions for the specified IP address. The LDP sessions are automatically reestablished when at least one Hello adjacency exists with the neighbor, and the LDP configuration remains unchanged.

Syntax

clear mpls ldp neighbor { all | peer-ip-addr [ label-space-id label-space ]}

Parameters

all
All LDP sessions on the Brocade device are reset, including the targeted LDP sessions.

peer-ip-addr
An LDP session. All LDP sessions with the matching peer address is reset.

label-space-id label-space
Specifies the label space for the LDP session.

Modes

Privileged EXEC mode

Usage Guidelines

This command allows you to reset the following LDP sessions:

- Platform-wide label space
- Interface specific label space

When an LDP session is terminated as a result of the clear mpls ldp neighbor command, the Brocade device does not generate any notification message for the neighbor. Instead, the device unilaterally terminates the session and closes the associated TCP session. The other end of the LDP session detects this reset operation in either of the following two ways:

- TCP session is broken (half connected). The device detects this while receiving or sending LDP messages on TCP socket fails (with fatal error), indicating that underlying TCP session is aborted by remote peer.
- A new TCP connection request is received from the neighbor while the older session is still operational (when this is in the passive role).

NOTE
Either of the previous events trigger the remote end of the LDP session to tear down the session and try to reestablish it. Resetting an LDP session impacts the associated VPLS or VLL sessions. Resetting an LDP session which is not in an operational state has no impact.

When the LDP session is not found corresponding to the specified peer-ip-addr and, if applicable, label-space, a warning message is displayed.

When an LDP session is not in operational state, resetting it has no impact.
When the **all** option is specified, all LDP sessions on the Brocade device is reset, including the targeted LDP sessions.

### Examples

The following example clears both the link and targeted LDP session with neighbor 10.234.123.64 because the `label_space` optional parameter has not been specified.

```plaintext
device# clear mpls ldp neighbor 10.234.123.64
device#
```
clear mpls ldp statistics
Clears the LDP packet statistics displayed by the show mpls ldp statistics command.

Syntax
clear mpls ldp statistics

Modes
Privileged EXEC mode

Usage Guidelines
This command clears packet statistics including packet types and packet errors.

Examples
The following example clears the LDP packet statistics.

device# clear mpls ldp statistics
clear mpls rsvp statistics session

Clears RSVP session statistics.

Syntax

clear mpls rsvp statistics session { [ [ destination ip_addr ] ] [ source source_ip ] [ tunnel-id tunnel_id lsp-id lsp_id ] } | { name session_name } | { p2mp p2mp-id [ ip_addr | dec ] } [ source source_ip ] [ tunnel-id tunnel_id lsp_id ]

Parameters

destination ip_addr
Defines the destination IP address.

source source_ip
Defines the source IP address.

tunnel tunnel_id
Defines the tunnel by decimal number 1 - 65535.

lsp-id lsp_id
Defines the LSP by decimal number 1 - 65535.

name session_name
Clears the session by name.

p2mp p2mp-id
Clears the point to multipoint sessions.

ip_addr
Specifies the P2MP identifier as an IP address

dec
Specifies the P2MP identifier as a decimal.

Modes

Privileged EXEC mode.

Usage Guidelines

This command operates in all modes.

Examples

The following example clears the RSVP session statistics for the lsp_test session.

device(config)# clear mpls rsvp statistics session
device(config)# clear mpls rsvp statistics session destination 11.11.11.11
device(config)# clear mpls rsvp statistics session destination 11.11.11.11 source 14.14.14.14
device(config)# clear mpls rsvp statistics session destination 11.11.11.11 source 14.14.14.14 tunnel-id 10
device(config)# clear mpls rsvp statistics session name lsp_test
device(config)# clear mpls rsvp statistics session p2mp p2mp-id 1.1.1.1 source 1.1.1.1 tunnel-id 1
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to provide the same statistics that are available at the global and interface level at the per-session level.</td>
</tr>
</tbody>
</table>
**clear mpls statistics**

Clears MPLS statistics.

```
clear mpls statistics 6pe [ slot/port | vrf ]
clear mpls statistics bypass-lsp lsp_name
clear mpls statistics label [ num | slot/port ]
clear mpls statistics ldp [ transit | tunnel ]
clear mpls statistics lsp lsp_name
clear mpls statistics oam
clear mpls statistics rsvp [ neighbor | session ]
clear mpls statistics tunnel num
clear mpls statistics vil [ vil_id | vil_name ]
clear mpls statistics vil-local [ vil_local_id | vil_local_name ]
clear mpls statistics vpls [ vpls_id | vpls_name ]
clear mpls statistics vrf vrf_name
```

**Parameters**

**6pe**

Clears 6pe statistics.

- **slot/port**
  
  Interface slot and port number.

- **vrf**
  
  Clears IPv6 VRF statistics.

**bypass-lsp**

Clears statistics for bypass LSPs.

- **lsp_name**
  
  Name of targeted LSP.

**label**

Clears in-label statistics.

- **num**
  
  In-label.

  - **slot/port**
    
    Interface number.

**ldp**

Clears ingress tunnel accounting for LDP signaled LSP.

**transit**

Clears transit traffic statistics for LDP.
tunnel
  Clears ingress tunnel accounting for LDP created tunnels.

lsp
  Clears ingress tunnel accounting for RSVP signaled LSP.
  lsp_name
    Name of targeted LSP.

oam
  Clears OAM statistics.

rsvp
  Clears transit statistics for RSVP signaled LSP.
  neighbor
    Clears statistics for RSVP neighbor.
  session
    Clears transit statistics for RSVP sessions.

tunnel
  Clears MPLS tunnel statistics.
  num
    Tunnel interface index.

vll
  Clears VLL statistics.
  vll_id
    VLL identifier.
  vll_name
    Name of VLL.

vll-local
  Clears VLL local statistics.
  local_vll_id
    Local VLL identifier.
  local_vll_name
    Name of local VLL.

vpls
  Clears VPLS statistics.
  vpls_id
    VPLS identifier.
  vpls_name
    Name of VPLS.

vrf
Clears VRF statistics.

`vrf_name`
Name of VRF.

**Modes**
Privileged EXEC mode.

**Examples**
The following example clears bypass LSPs statistics:

```
device# clear mpls statistics bypass-lsp
Cleared statistics of bypass LSPs
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was modified to include the <code>bypass-lsp</code> keyword.</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIO5.5.00c</td>
<td>This command was modified to delete a single flow on a specified flow-id or all flow deletion in the flow table.</td>
</tr>
</tbody>
</table>
clear pki counters
Clears the Public Key Infrastructure (PKI) counters for a certificate authority (CA).

Syntax

clear pki counters

Modes

PKI trustpoint configuration mode.

Examples

The following example clears the PKI counters for the CA.

device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# clear pki counters

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear pki crl

Removes the certificate revocation list (CRL) database for a specific trustpoint name.

Syntax

```
clear pki crl trustpoint name
```

Parameters

*trustpoint name*

 Specifies the trustpoint name whose CRL database has to be removed.

Modes

PKI trustpoint configuration mode.

Examples

The following example removes the CRL database for the specified trustpoint name.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# clear pki crl Trustpoint1
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

Netiron Command Line Interface (CLI) Reference Guide
53-1004199-02

159
clear rate-limit counters bum-drop

Clears the accounting information for the Broadcast, Unicast, Multicast (BUM) traffic rate limit.

Syntax

clear rate-limit counters bum-drop [portid] [vlanid]
clear rate-limit counters bum-drop [shutdown] [portid] slot/port [all] [vlan-id] [vlan]

Parameters

portid
Optionally clears the accounting information for BUM rate-limiting for the specified port.

vlanid
Optionally clears the accounting information for BUM rate-limiting for the specified VLAN.

Modes

Privileged EXEC configuration mode

Usage Guidelines

This command is used to clear rate-limiting accounting information for BUM traffic and, optionally, for specified interfaces or VLANs.

Examples

The following example clears the BUM rate-limiting information for VLAN 2.

device# clear rate-limit counters bum-drop vlan2

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear rate-limit counters ip-option-pkt-to-cpu

Clears the rate-limit counters for IPv4 option packets.

Syntax

clear rate-limit counters ip-option-pkt-to-cpu

Modes

This command operates in all mode.

Examples

The following example shows how to clear the rate-limit counters for IPv4 option packets.

Brocade# clear rate-limit counters ip-option-pkt-to-cpu

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Service IronWare Release 5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear rate-limit counters ipv6-hoplimit-expired-to-cpu
Cleans the rate-limit counters for IPv6 hoplimit-expired-to-cpu packets.

Syntax

    clear rate-limit counters ipv6-hoplimit-expired-to-cpu

Modes
This command operates in all mode.

Examples
The following example shows how to clear the rate-limit counters for hoplimit-expired-to-cpu packets.

    Brocade# clear rate-limit counters ipv6-hoplimit-expired-to-cpu

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Service IronWare Release 5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
clear rate-limit counters ip-ttl-expired-to-cpu

Clears the rate-limit counters for IPv4 ttl-expired-to-cpu packets.

Syntax

    clear rate-limit counters ip-ttl-expired-to-cpu

Modes

This command operates in all mode.

Examples

The following example shows how to clear the rate-limit counters for ip-ttl-expired-to-cpu.

    Brocade# clear rate-limit counters ip-ttl-expired-to-cpu

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Service IronWare Release 5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>NI05.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**client-interfaces sync_ccep_early**

Adds a time delay before the Cluster Client Edge Port (CCEP) goes to the forwarding state.

**Syntax**

```
client-interfaces sync_ccep_early lacp-delay value
no client-interfaces sync_ccep_early lacp-delay value
```

**Command Default**

There is no time delay set when Link Aggregation Control Protocol (LACP) is in the blocked state.

**Parameters**

- `lacp-delay`
  - Configures a time delay for the LACP blocked state.
- `value`
  - Specifies the time delay value in seconds. The valid values are from 3 through 10 seconds. The default value is 3 seconds.

**Modes**

MCT cluster configuration mode

**Usage Guidelines**

The command enables faster synchronization of the CCEP *up or down* state to the MCT node.

**NOTE**

Configure this command only when required because there may be high broadcast, unknown unicast and multicast (BUM) traffic drops due to this configuration.

The *no* form of the command removes the predefined time delay for the LACP blocked state.

**Examples**

The following example sets a time delay of 8 seconds before the CCEP goes to the forwarding state for the MCT cluster "abc".

```
device(config)# cluster abc 1
device(config-cluster-abc)# client-interfaces sync_ccep_early lacp-delay 8
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
cluster-client-static-mac-move

Enables the static MAC address movement from the local Cluster Client Edge Port (CCEP) to the Inter-Chassis Link (ICL) port in the MAC cluster and vice versa.

Syntax

cluster-client-static-mac-move
no cluster-client-static-mac-move

Modes

MCT cluster configuration mode

Usage Guidelines

This command must be configured in both the MCT peers but the static MAC address under the VLAN must be configured on any one of the MCT peers.

The no form of the command disables the static MAC address movement from the local CCEP to the ICL port.

Examples

The following example enables the static MAC address movement from the local CCEP to the ICL port (and vice versa) in the MAC cluster named "brocade" with the cluster ID set as 1.

device(config)# cluster brocade 1
device(config-cluster-brocade)# cluster-client-static-mac-move

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**cluster-id**

Configures a cluster ID for the route reflector.

**Syntax**

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

**Command Default**

The default cluster ID is the device ID.

**Parameters**

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

- **ip-addr**
  
  IPv4 address in dotted-decimal notation.

**Modes**

BGP configuration mode

**Usage Guidelines**

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

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

**Examples**

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

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

Copies a file from a source device to a destination server (usually remote) or from a server (source) to a Brocade device (destination). This command can also be used to upload or download a configuration file. Each syntax instance is slightly different for the various operations.

**Syntax**

```plaintext
copy source protocol { ipv4-address | ipv6-address } [ public-key { dsa | rsa } ] [ remote-port ] remote-filename device-filename

copy protocol destination { ipv4-address | ipv6-address } [ public-key { dsa | rsa } ] [ remote-port ] remote-filename device-filename

copy config-file protocol { ipv4-address | ipv6-address } [ public-key { dsa | rsa } ] [ remote-port ] remote-filename

copy protocol config-file { ipv4-address | ipv6-address } [ public-key { dsa | rsa } ] [ remote-port ] remote-filename
```

**Parameters**

<table>
<thead>
<tr>
<th><strong>source</strong></th>
<th>Specifies the location of the file on the source device to be copied to the server. Can be one of the following: <code>flash</code>, <code>scp</code>, <code>slot1</code>, or <code>slot2</code> depending on the device. CES and CER devices support only the <code>flash</code> option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protocol</strong></td>
<td>Specifies the protocol to be used. Can be one of the following: <code>flash</code>, <code>http</code>, <code>https</code>, or <code>scp</code>.</td>
</tr>
<tr>
<td><strong>destination</strong></td>
<td>Specifies the location on the destination device where the file is to be copied from the server. Can be one of the following: <code>flash</code>, <code>scp</code>, <code>slot1</code>, <code>slot2</code>, depending on the device. CES and CER devices support only the <code>flash</code> option.</td>
</tr>
<tr>
<td><strong>ipv4-address</strong></td>
<td>Specifies the IPv4 address of the server.</td>
</tr>
<tr>
<td><strong>ipv6-address</strong></td>
<td>Specifies the IPv6 address of the server.</td>
</tr>
<tr>
<td><strong>remote-filename</strong></td>
<td>Specifies the name of the file to be used on the remote server. You can specify up to 127 characters for the file name.</td>
</tr>
<tr>
<td><strong>device-filename</strong></td>
<td>Specifies the name of the file to be used on the local device. Certain filenames are reserved and the system will not allow you to use them.</td>
</tr>
<tr>
<td><strong>config-file</strong></td>
<td>Specifies the configuration file to be used. Can be either <code>running-config</code> or <code>startup-config</code>.</td>
</tr>
</tbody>
</table>

**Modes**

Privileged EXEC mode
Usage Guidelines

You are prompted for *username* and *password* when you execute this command. The maximum length is 48 characters for each.

Please note that each syntax instance is different and is used to perform the following actions:

- Upload a copy of a file from a Brocade device (source) using a specified protocol to a server (destination) using the first syntax
- Download a copy of a file from a server (destination) using a specified protocol to a Brocade device (source) using the second syntax
- Upload a configuration file using the third syntax
- Download a configuration file using the fourth syntax

**NOTE**

When downloading a file to flash, the destination filename cannot be same as any of the reserved file names in flash. CLI will throw the following error when destination filename is any of the reserved file name: Error: Destination file name(%s) cannot be same as any of the reserved file names in flash.

Examples

The following example uploads a copy of an OS image file from the primary flash memory on a device to an SCP server with the IP address of 172.26.51.180:

```
device# copy scp slot1 172.26.51.180 public-key dsa image-filename primary
```

The following example downloads a copy of an file from an SCP server to a Brocade device with the IP address of 10.20.99.146

```
device# copy flash scp 10.20.99.146 ~/xmr05800.bin primary
```

The following example uploads a copy of the image file "startup-config" from the primary flash memory on a device to a file named "startup-config-srv.txt" on an HTTP server with the IP address of 172.26.51.180:

```
device# copy flash http 172.26.51.180 startup-config-srv.txt startup-config
```

The following example downloads a copy of the image file "startup-config-srv.txt" from the HTTP server with the IP address of 172.26.51.180 to a "startup-config" file on slot2 of the device.

**NOTE**

When downloading, the system will not allow you to use certain filenames as a destination (target) filename.

```
device# copy http slot2 172.26.51.180 startup-config-srv.txt startup-config-dev.txt
```
**copy tftp license**

Copies the license file from the TFTP server to the license database of the Brocade device.

**Syntax**

```
copy tftp license { ip_address | ipv6_address } license_filename_on_host
```

**Command Default**

By default, the command is not enabled.

**Parameters**

- `ip_address`  
  Specifies the address of the IPv4 TFTP server.

- `ipv6_address`  
  Specifies the address of the IPv6 TFTP server.

- `license_filename_on_host`  
  Specifies the filename of the license file.

**Modes**

Privileged EXEC level.

**Usage Guidelines**

To remove a license file, use the `license delete` command.

If you attempt to download the same license twice on the device, the following error message is displayed on the console.

Can’t add the license string - 93 (DUPLICATE_LICENSE)

**Examples**

The following example copies the license file from the TFTP server to the license database of the Brocade device.

```
device# copy tftp license 10.1.1.1 lic.xml
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>07.1.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
copy-received-cos
Classifies and prioritizes the management traffic for QoS.

Syntax
  copy-received-cos protocol

Parameters
  SSH
    Specifies the SSH protocol.
  Telnet
    Specifies the Telnet protocol.

Modes

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**common-name**

Specifies the common name parameter for the Public Key Infrastructure (PKI) entity.

**Syntax**

```
common-name name
```

**Parameters**

*name*

Specifies the common name parameter for the PKI entity.

**Modes**

PKI entity configuration mode

**Examples**

The following example specifies the common name parameter for the PKI entity.

```
device(config)# pki entity brocade_entity
device(config-pki-entity-brocade_entity)# common-name brocade_e
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**compare-med-empty-aspath**

Enables comparison of Multi-Exit Discriminators (MEDs) for internal routes that originate within the local autonomous system (AS) or confederation.

**Syntax**

```plaintext
compare-med-empty-aspath
no compare-med-empty-aspath
```

**Modes**

BGP configuration mode

**Usage Guidelines**

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

**Examples**

This example configures the device to compare MEDs:

```plaintext
device# configure terminal
device(config)# router bgp
device(config-bgp)# compare-med-empty-aspath
```
**compare-routerid**

Enables comparison of device IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

**Syntax**

```markdown
compare-routerid
no compare-routerid
```

**Command Default**

This feature is disabled.

**Modes**

- BGP configuration mode

**Usage Guidelines**

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

**Examples**

This example configures the device always to compare device IDs.

```bash
device# configure terminal
device(config)# router bgp
device(config-bgp)# compare-routerid
```
confederation identifier

Configures a BGP confederation identifier.

Syntax

confederation identifier autonomous-system number

no confederation identifier

Command Default

No BGP confederation identifier is identified.

Parameters

autonomous-system number

Specifies an autonomous system number (ASN). The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

Use the no form of this command to remove a BGP confederation identifier.

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

Examples

This example specifies that confederation 65220 belongs to autonomous system 100.

device# configure terminal
device(config)# router bgp
device(config-bgp)# local-as 65220
device(config-bgp)# confederation identifier 100
confederation peers

Confines 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-router)# local-as 65020
device(config-router)# confederation identifier 100
device(config-router)# confederation peers 65520 65521 65522
country-name

Configures the country code for the Public Key Infrastructure (PKI) entity.

Syntax

country-name name

Parameters

name

Specifies the country code for the PKI entity.

Modes

PKI entity configuration mode

Usage Guidelines

The country code is specified as a standard two-character code for a country. For example, IN can be the country code for India and US for United States of America.

Examples

The following example configures the India country code for the PKI entity.

device(config)# pki entity brocade_entity
device(config-pki-entity-brocade_entity)# country-name IN

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**crl-query**
Sets the certificate revocation list (CRL) URL name if the revocation check is configured as CRL in the device.

**Syntax**

```
crl-query URL name
no crl-query URL name
```

**Parameters**

- **URL name**
  The CRL URL name.

**Modes**

PKI trustpoint configuration mode.

**Usage Guidelines**

The **no** form of the command removes the specified CRL URL name.

**Examples**

The following example specifies the CRL URL name as provided.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# crl-query http://WIN-HJ98AK136A0.englab.brocade.com/CertEnroll/englab-WIN-HJ98AK136A0-CA-7.crl
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
crl-update-time

Sets the certificate revocation list (CRL) update period for a certificate.

Syntax

crl-update-time hours
no crl-update-time hours

Command Default

The CRL update period depends on the next update field in the CRL file.

Parameters

hours

The CRL update period value in hours. Valid values range from 1 through 1000 hours.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The no form of the command removes the specified CRL update time.

Examples

The following example specifies the CRL update time as 10 hours.

device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# crl-update-time 10

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
cspf-computation-mode

Configures the IS-IS ignore overload bit.

Syntax

cspf-computation-mode [ ignore-overload-bit | use-bypass-liberal | use-bypass-metric | use-igp-metric | use-te-metric ]

no cspf-computation-mode [ ignore-overload-bit | use-bypass-liberal | use-bypass-metric | use-igp-metric | use-te-metric ]

Command Default

By default, this command is disabled.

Parameters

ignore-overload-bit

Ignores the overload bit during CSPF computation.

use-bypass-liberal

Uses the liberal mode for CSPF facility backup computation.

use-bypass-metric

Uses the bypass LSPs path for cost for selection between bypass LSPs.

use-igp-metric

Uses the IGP metric of the link for CSPF computation.

use-te-metric

Uses the TE metric of the link for CSPF computation.

Modes

MPLS policy configuration mode

Usage Guidelines

The no form of the command allows CSPF to reject the path transiting through and overloaded router from the ingress.

Configuring this command will indicate that all the future CSPF calculations through an overloaded transit router are not rejected.

Because the command is at the global level, it will affect all the LSPs.
Examples

The following example configures the software to ignore the overload bit during CSPF computation. The output of the `show mpls config` command verifies the configuration.

device(config-mpls-policy)# cspf-computation-mode ignore-overload-bit
device(config-mpls-policy)# show mpls config
router mpls
  policy
    traffic-eng isis level-1
    handle-isis-neighbor-down
    cspf-computation-mode ignore-overload-bit

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
cspf-computation-mode (LSP level)

Configures the CSPF computation mode for RSVP LSPs.

Syntax

cspf-computation-mode \[ use-igp-metric | use-te-metric \]

no cspf-computation-mode \[ use-igp-metric | use-te-metric \]

Command Default

By default, LSP uses the CSPF computation mode from the global configuration at MPLS policy level.

Parameters

use-igp-metric

Uses the IGP metric of the link for CSPF computation.

use-te-metric

Uses the TE metric of the link for CSPF computation

Modes

Primary, secondary, and at static bypass LSP context level under the router MPLS mode.

Usage Guidelines

The **cspf-computation-mode** command configures the computation mode for CSPF to use TE-metric or IGP-metric at primary, secondary, and static bypass LSP levels by overriding global LSP configuration.

The **no** version of this command will set the CSPF computation to use the global configuration from router MPLS policy level.

Examples

The following example explains configuration of CSPF computation mode to use TE-metric or IGP-metric at LSP level.

```
device(config)# router mpls
device(config-mpls)# lsp test
device(config-mpls-lsp-test)# cspf-computation-mode ?
  use-igp-metric       use IGP metric of the link for CSPF computation
  use-te-metric        use TE metric of the link for CSPF computation

device(config-mpls-lsp-test)# cspf-computation-mode use-igp-metric
device(config-mpls-lsp-test)# cspf-computation-mode use-te-metric
Error:CSPF computation is configured to use igp-metric
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
database-overflow-interval (OSPFv3)

Configures frequency for monitoring database overflow.

Syntax

```
database-overflow-interval interval
no database-overflow-interval
```

Command Default

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

Parameters

```
interval
```

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds (24 hours).

Modes

OSPFv3 router configuration mode
OSPFv3 router VRF configuration mode

Usage Guidelines

This command specifies how long after a router that has entered the OverflowState before it can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the `external-lsdb-limit` CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

If the configured value of the database overflow interval is 0, then the device never leaves the database overflow condition.

The `no` form of the command disables the overflow interval configuration.

Examples

The following example configures a database-overflow interval of 120 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# database-overflow-interval 120
```
**dead-interval**

Configures the interval for which a Virtual Router Redundancy Protocol (VRRP) backup router waits for a hello message from the VRRP master router before determining that the master is offline. When backup routers determine that the master is offline, the backup router with the highest priority becomes the new VRRP master router.

**Syntax**

```
dead-interval [ msec ] interval
no dead-interval [ msec ] interval
```

**Command Default**

The default dead interval is internally derived from the hello interval. It is equal to 3 times the hello interval plus the skew time, where the skew time is equal to (256 minus the priority) divided by 256.

**Parameters**

- **msec interval**
  
  Sets the interval, in milliseconds, for which a VRRP backup router waits for a hello message from the VRRP master router before determining that the master is offline. Valid values range from 100 through 84000. The default value is 1000. VRRP-E does not support the dead interval in milliseconds.

- **interval**
  
  Sets the interval, in seconds, for which a VRRP backup router waits for a hello message from the VRRP master router before determining that the master is offline. Valid values range from 1 through 84. The default value is 1.

**Modes**

VRID interface configuration mode

**Usage Guidelines**

By default, the dead interval is internally derived from the hello interval. It is equal to 3 times the hello interval plus the skew time, where the skew time is equal to (256 minus the priority) divided by 256. Generally, if you change the hello interval on the VRRP master device using the `hello-interval` command, you should also change the dead interval on the VRRP backup devices using the `dead-interval` command.

A VRRP master router periodically sends hello messages to the backup routers. The backup routers use the hello messages as verification that the master is still online. If the backup routers stop receiving the hello messages for the period of time specified by the dead interval, the backup routers determine that the master router is offline. At that point, the backup router with the highest priority becomes the new master router.

The `dead-interval` command is configured only on VRRP backup routers and is supported by VRRP and VRRP-E.

The `no` form resets the dead interval to its default value of 1000 milliseconds (1 second).

**NOTE**

VRRP-E does not support the hello message interval in milliseconds.
Examples

The following example sets a waiting period of 25000 milliseconds before a VRRP backup router determines that a VRRP master router is offline.

device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# backup priority 40 track-priority 10
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.99
device(config-if-e1000-1/6-vrid-1)# dead-interval msec 25000
device(config-if-e1000-1/6-vrid-1)# activate

The following example sets a waiting period of 25 seconds before a VRRP-E backup router determines that a VRRP master router is offline.

device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(conf-if-e1000-1/5)# ip address 10.53.5.3/24
device(conf-if-e1000-1/5)# ip vrrp-extended vrid 2
device(conf-if-e1000-1/5-vrid-2)# backup priority 50 track-priority 10
device(conf-if-e1000-1/5-vrid-2)# ip-address 10.53.5.1
device(conf-if-e1000-1/5-vrid-2)# dead-interval 25
device(conf-if-e1000-1/5-vrid-2)# activate
default-link-metric

Configures the metric value globally on all active IPv4 IS-IS interfaces.

Syntax

default-link-metric value [ level-1 | level-2 ]

no default-link-metric value [ level-1 | level-2 ]

Command Default

The default-link-metric command is disabled by default.

Parameters

default-link-metric value

Specifies the global default-link-metric parameter for an IPv4 IS-IS unicast address family configuration.

value

Specifies the default-link-metric value in metric style and configurable range. The metric style consists of narrow or wide style. The narrow metric range is from 1 - 63. The wide metric range is from 1 - 16777215. If you change the metric style configuration, the default-link-metric value will also change. The new default-link-metric value is equal to the minimum of the configured value, and the maximum value supported by the new metric style. For example, if the metric style changes from a wide metric to a narrow metric, and the default-link-metric value is greater than 63, the default-link-metric value changes to 63 because it is the maximum value supported in the narrow metric style. When the metric style changes from a narrow metric to a wide metric, there is no change to the default-link-metric value.

level-1 | level-2

Specifies the IS-IS routing parameter as level-1 or level-2. You can choose to configure the default-link-metric parameter as either level-1 or level-2. If the IS-IS routing parameter is not configured, the default-link-metric value is applied to both level-1 and level-2.

Modes

IPv4 IS-IS unicast address family configuration level.

Usage Guidelines

Use the default-link metric value command to change the metric value globally on all active IPv4 IS-IS interfaces. The default-link metric value command is useful when you have a common IS-IS metric value on all IS-IS interfaces, other than the default metric value of 10. The command enables the metric value for IPv4 routes per address family configuration. Use the no form of the command to reset the metric value to the default value 10. The default-link metric value command is not applicable to MPLS IS-IS shortcuts and tunnel interfaces.

You can change the metric value for a specific interface using the isis metric command or the isis ipv6 command. The isis metric command configuration takes precedence over the default-link metric value command configuration.

During switchover or hitless upgrade, the IS-IS default link metric configuration is not affected. Backward compatibility is not supported.

NOTE

The default-link metric value command is supported on the Brocade NetIron XMR Series, the Brocade MLX Series, and the Brocade NetIron CER Series and Brocade NetIron CES Series platforms.
Examples

The following example configures the IS-IS default link metric value to 30 for an IPv4 address family. The default-link-metric value of 30 is applied to both level-1 and level-2.

```
device(config)# router isis
device(config-isis-router)# address-family-ipv4 unicast
device(config-isis-router-ipv4u)# default-link-metric 30
```

The following example configures the IS-IS default link metric value to 30 for level-1, and the IS-IS default link metric value of 40 to level-2.

```
device(config)# router isis
device(config-isis-router)# address-family-ipv4 unicast
device(config-isis-router-ipv4u)# default-link-metric 30 level-1
device(config-isis-router-ipv4u)# default-link-metric 40 level-2
```

Use the `show isis` command to display the configuration for the IS-IS default link metric value.

```
device(config)# show isis
....
Default redistribution metric: 0
Default link metric for level-1: 33 (conf)/ 33 (adv)
Default link metric for level-2: 5 (conf)/ 5 (adv)
Protocol Routes redistributed into IS-IS:
....
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**default-local-preference**

Enables setting of a local preference value to indicate a degree of preference for a route relative to that of other routes.

**Syntax**

```
default-local-preference num
no default-local-preference
```

**Command Default**

The default local preference is 100.

**Parameters**

`num`

Local preference value. Range is from 0 through 4294967295.

**Modes**

BGP configuration mode

**Usage Guidelines**

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

Use this command to change the local preference value. Local preference indicates a degree of preference for a route relative to that of other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message.

**Examples**

This example sets the local preference value to 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# default-local-preference 200
```
**default-metric (OSPF)**

Sets the default metric value for the OSPFv2 or OSPFv3 routing protocol.

**Syntax**

```
default-metric metric
no default-metric
```

**Command Default**

The default metric value for the OSPFv2 or OSPFv3 routing protocol is 10.

**Parameters**

- `metric`
  
  OSPF routing protocol metric value. Valid values range from 1 through 65535.

**Modes**

- OSPF router configuration mode
- OSPFv3 router configuration mode
- OSPF router VRF configuration mode
- OSPFv3 router VRF configuration mode

**Usage Guidelines**

This command overwrites any incompatible metrics that may exist when OSPFv2 or OSPFv3 redistributes routes. Therefore, setting the default metric ensures that neighbors will use correct cost and router computation.

The `no` form of the command restores the default setting.

**Examples**

The following example sets the default metric to 20 for OSPF.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# default-metric 20
```
default-passive-interface
Marks all OSPFv2 and OSPFv3 interfaces passive by default.

Syntax

\begin{verbatim}
  default-passive-interface
  no default-passive-interface
\end{verbatim}

Modes

- OSPF router configuration mode
- OSPFv3 router configuration mode
- OSPF router VRF configuration mode
- OSPFv3 router VRF configuration mode

Usage Guidelines

When you configure the interfaces as passive, the interfaces drop all the OSPFv2 and OSPFv3 control packets.

You can use the `ip ospf active` and `ip ospf passive` commands in interface subconfiguration mode to change active/passive state on specific OSPFv2 interfaces. You can use the `ipv6 ospf active` and `ipv6 ospf passive` commands in interface subconfiguration mode to change the active and passive state on specific OSPFv3 interfaces.

The `no` form of the command disables the passive state.

Examples

The following example marks all OSPFv2 interfaces as passive.

\begin{verbatim}
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# default-passive-interface
\end{verbatim}

The following example marks all OSPFv3 interfaces as passive for VRF “red”.

\begin{verbatim}
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ospf6-router-vrf-red)# default-passive-interface
\end{verbatim}
**delete-certificate**

Deletes all the trustpoint certificates or a specific certificate associated with a trustpoint.

**Syntax**

```
delete-certificate [ certificate-serial-number ]
```

**Parameters**

- `certificate-serial-number` Specifies the serial number of the certificate.

**Modes**

PKI trustpoint configuration mode.

**Usage Guidelines**

When the local certificate is deleted, the existing established IKEv2 SA are not affected but any new IKEv2 SA establishment is not allowed if x509v3 certificate is needed for authentication.

**NOTE**

This command is applicable only for certificates downloaded from CA server.

**Examples**

The following example deletes a specific trustpoint certificate.

```
device(config)# pki-trustpoint test
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
diagnostics (MRP)
   Enables diagnostics on a metro ring.

Syntax
   diagnostics
   no diagnostics

Command Default
   Diagnostics are disabled by default.

Modes
   Metro ring configuration mode

Usage Guidelines
   This command is valid only on the master node.

   When you enable Metro Ring Protocol (MRP) diagnostics, the software tracks Ring Health Packets (RHPs) according to their sequence numbers and calculates how long it takes an RHP to travel one time through the entire ring. The calculated results have a granularity of 1 microsecond. When you display the diagnostics, the output shows the average round-trip time for the RHPs sent since you enabled diagnostics.

   The no form of the command disables the diagnostics for the ring.

Examples
   The following example enables the diagnostics for metro ring 1.

   device(config)# vlan 2
   device(config-vlan-2)# metro-ring 1
   device(config-vlan-2-mrp-1)# diagnostics
disable authenticate md5
  Disables the MD5 authentication scheme for Network Time Protocol (NTP).

Syntax
  disable authenticate md5
  no disable authenticate md5

Command Default
  If JITC is enabled, the MD5 authentication scheme is disabled. In the standard mode, the MD5 authentication scheme is enabled.

Modes
  NTP configuration mode.

Usage Guidelines
  In the standard mode, both SHA1 and MD5 authentication schemes are supported. If JITC is enabled using the jitc enable command, the MD5 authentication for Network Time Protocol (NTP) is disabled by default and the disable authenticate md5 command can be seen in the running configuration. In the JITC mode, only the SHA1 authentication option is available. The SHA1 authentication scheme must be enabled manually by configuring the authentication key for NTP using the authentication-key command and an example of configuring this command is shown below.

  The no form of the command enables the MD5 authentication scheme.

Examples
  The following example disables the MD5 authentication scheme.
  
  device# configure terminal
  device(config)# ntp
  device(config-ntp)# disable authenticate md5

  The following example enables SHA1 authentication for NTP.
  
  device# configure terminal
  device(config)# ntp
  device(config-ntp)# authentication-key key-id 20 sha1 keystring

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
disable-acl-for-6to4

Disables IPv6 access control list (ACL) processing for IPv6-over-IPv4 internal traffic.

Syntax

disable-acl-for-6to4

no disable-acl-for-6to4

Command Default

ACL processing is enabled for IPv6-over-IPv4 traffic.

Modes

ACL policy configuration mode

Usage Guidelines

This command only affects a tunnel-terminating node.

The command does not affect the following types of ACLs:

- Layer 2 (MAC) ACLs
- IPv4 ACLs
- User-defined ACLs (UDA ACLs)

Disabling ACL processing also disables support for the following features for internal traffic coming over the tunnel:

- All features employing IPv6 ACLs
- BFD over MPLS
- Multicast
- PBR
- OpenFlow

The no form of this command re-enables ACL processing.

Examples

The following example disables IPv4 and IPv6 ACL processing on a tunnel-terminating node.

device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# disable-acl-for-6to4

The following example re-enables ACL processing.

device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# no disable-acl-for-6to4
# History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Netiron Command Line Interface (CLI) Reference Guide
S3-1004199-02

195
disable-acl-for-gre

Disables IPv4 and IPv6 access control list (ACL) processing for Generic Routing Encapsulation (GRE)-tunneled internal traffic.

Syntax

disable-acl-for-gre

no disable-acl-for-gre

Command Default

ACL processing is enabled for GRE-tunneled traffic.

Modes

ACL policy configuration mode

Usage Guidelines

This command only affects a tunnel-terminating node.

The command does not affect the following types of ACLs:

- Layer 2 (MAC) ACLs
- User-defined ACLs (UDA ACLs)

This command applies to both named and numbered ACLs.

Disabling ACL processing also disables support for the following features for internal traffic coming over the tunnel:

- All features employing IPv4/IPv6 ACLs
- BFD over MPLS
- Multicast
- PBR
- OpenFlow

The no form of this command re-enables ACL processing.

Examples

The following example disables IPv4 and IPv6 ACL processing on a tunnel-terminating node.

device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# disable-acl-for-gre

The following example re-enables ACL processing.

device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# no disable-acl-for-gre
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

NetIron Command Line Interface (CLI) Reference Guide
53-1004199-02
**distance (BGP)**

Changes the default administrative distances for eBGP, iBGP, and local BGP.

**Syntax**

```
distance external-distance internal-distance local-distance

no distance
```

**Command Default**

**Parameters**

- `external-distance`
eBGP distance. Range is from 1 through 255.

- `internal-distance`
iBGP distance. Range is from 1 through 255.

- `local-distance`
Local BGP4 and BGP4+ distance. Range is from 1 through 255.

**Modes**

BGP configuration mode

**Usage Guidelines**

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

To select one route over another according to the source of the route information, the device can use the administrative distances assigned to the sources. The administrative distance is a protocol-independent metric that IP devices use to compare routes from different sources. Lower administrative distances are preferred over higher ones.

**Examples**

This example configures the device to change the administrative distance.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# distance 100 150 200
```
distance (OSPF)

Configures an administrative distance value for OSPFv2 and OSPFv3 routes.

Syntax

distance { external | inter-area | intra-area } distance

no distance

Command Default

The administrative distance value for OSPFv2 and OSPFv3 routes is 110.

Parameters

external
Sets the distance for routes learned by redistribution from other routing domains.

inter-area
Sets the distance for all routes from one area to another area.

intra-area
Sets the distance for all routes within an area.

distance
Administrative distance value assigned to OSPF routes. Valid values range from 1 through 255. The default is 110.

Modes

OSPF router configuration mode
OSPFv3 router configuration mode
OSPF router VRF configuration mode
OSPFv3 router VRF configuration mode

Usage Guidelines

You can configure a unique administrative distance for each type of OSPF route.

The distances you specify influence the choice of routes when the device has multiple routes from different protocols for the same network. The device prefers the route with the lower administrative distance. However, an OSPFv2 or OSPFv3 intra-area route is always preferred over an OSPFv2 or OSPFv3 inter-area route, even if the intra-area route's distance is greater than the inter-area route's distance.

The no form of the commands reverts to the default setting.
Examples

The following example sets the distance value for all external routes to 125.

device# configure terminal
device(config)# router ospf
device(config-ospf-router)# distance external 125

The following example sets the distance value for intra-area routes to 80.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# distance intra-area 80

The following example sets the distance value for inter-area routes to 90.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# distance inter-area 90
**display-pkt-bit-rate**

Displays the Packet and Bit rate statistics for the policy based routing.

**Syntax**

```
display-pkt-bit-rate

no display-pkt-bit-rate
```

**Command Default**

None.

**Modes**

- ACL policy sub-configuration mode (config-acl-policy).

**Usage Guidelines**

When deploying this command, a new display format displays the PBR statistics. Otherwise, the old or existing CLI display format is used (only packet rate statistics are displayed).

This configuration stores in the configuration file.

**Examples**

The following example shows how the new format can be enabled using the CLI command:

```
device(config-acl-policy) #display-pkt-bit-rate
```

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
**dot1ag-transparent**

Forwards non-CCM packets without altering the packet prioritization at the ingress.

**Syntax**

```
  dot1ag-transparent
  no dot1ag-transparent
```

**Command Default**

The command is not enabled by default.

**Modes**

Global configuration mode.

**Usage Guidelines**

When IEEE 802.1ag CFM is not configured for the device, the priority of non-CCM packets can change due to Protocol Packet Prioritization (PPP) at the ingress. Since the node needs to forward the packet without altering the packet priority, Brocade recommends using this command when forwarding non-CCM packets.

Theno form of the command reverts the command behavior back to default; non-CCM packets are forwarded with altered packet prioritization.

The command is saved upon reload.

**NOTE**

The command is supported on Brocade NetIron XMR Series and Brocade NetIron MLX Series devices.

**Examples**

The following example forwards the non-CCM packet without altering the packet priority.

```
device(config)# dot1ag-transparent
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**dot1x-key**

Configures switch port to dynamically obtain MKA keys from RADIUS server.

**Syntax**

```
dot1x-key
no dot1x-key
```

**Command Default**

By default, this command is disabled.

**Modes**

Macsec ethernet and group configuration mode

**Usage Guidelines**

The `dot1x-key` command is effective only if the interface is dot1x-enabled using the `dot1x-enable` command.

**NOTE**

An MKA configuration group should be attached to the interface before applying dot1x-key configuration on the interface.

The `no` form of the command disables dot1x-key configuration from the port.

**Examples**

The following example configures dot1x-key on Ethernet interface 1/1.

```
device# configure terminal
device(config)# dot1x-mka-enable
device(config)# dot1x-enable ethernet 1/1
device(config)# dot1x-key
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**dot1x-mka-enable**

Enables MACsec Key Agreement (MKA) capabilities on a Brocade device and enters dot1x-mka configuration mode.

**Syntax**

- `dot1x-mka-enable`
- `no dot1x-mka-enable`

**Command Default**

By default, MACsec MKA capabilities are not enabled.

**Modes**

Global configuration mode

**Usage Guidelines**

When the `dot1x-mka-enable` command is disabled, all the configurations under that mode are deleted. If MKA is disabled, all the ports go into a down state. To bring the ports back to online, you must manually enable each port.

The `no` form of this command disables the MKA and MACsec functionality on all ports.

**Examples**

The following example enables MACsec MKA capabilities is enabled on the device.

```plaintext
device# configure terminal
device(config)# dot1x-mka-enable
Brocade(config-dot1x-mka)#
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**eckeypair**

Specifies which Elliptic Curve key pair to use during enrollment.

**Syntax**

```
eckeypair { key-label label | encryption-key-size encryption key-size | key-size key-size }
```

**Parameters**

- `key-label label`
  Specifies the name of the key pair generated during enrollment. The name is specified if it is not already existing or if the `auto-enroll regenerate` command is configured.

- `encryption-key-size encryption key-size`
  Specifies the size of the second key that is generated to request separate encryption, signature keys, and certificates.

- `key-size key-size`
  Specifies the size of the desired EC key pair. If the key size is not specified, the existing key size is used. The supported values are 256 and 384.

**Modes**

- PKI trustpoint configuration mode

**Usage Guidelines**

The key pair is obtained by importing from the key file that has a specific label.

**Examples**

The following example specifies which EC key pair to use during enrollment.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# eckeypair key-label brocade
```

The following example specifies the encryption key size.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# eckeypair encryption-key-size 100
```

The following example specifies the desired EC key size of 256.

```
device(config)# pki-trustpoint test
device(config-pki-trustpoint-test)# eckeypair key-size 256
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.8.00b</td>
<td>This command was modified to add the <code>encryption-key-size</code> and <code>key-size</code> keywords.</td>
</tr>
</tbody>
</table>
**egress-truncate**

Enables the truncation of egress packets for a port.

**Syntax**

```plaintext
egress-truncate
no egress-truncate
```

**Command Default**

The command is not enabled by default. The specified size of the truncated packet is set globally using the `egress-truncate-size` command.

**Modes**

This command is used at the `config` level.

**Usage Guidelines**

The `no` form of the command disables truncation on the specific port. The `egress-truncate` command is supported for LAG ports.

**Examples**

The `egress-truncate-size` command enables truncation on all ports that are members of the LAG. The following example shows both LAG configuration and enabling truncate.

```plaintext
device(config)# lag lag1 static id 1
device(config-lag-lag1)# ports Ethernet 1/1 to 1/4
device(config-lag-lag1)# primary Ethernet 1/1
device(config-lag-lag1)# deploy

device(config-if-1/1)# egress-truncate
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**egress-truncate-size**
Sets the size of the truncated egress packets globally.

**Syntax**
```
egress-truncate-size value slot [all|slot_no [ <device_id>]]
no egress-truncate-size
```

**Command Default**
The command disabled by default. When enabled, the default setting is 64 bytes.

**Parameters**
- **value**
  The packet size in bytes after being truncated.
- **slot_no**
  An optional value for the slot number.
- **device_id**
  An optional value for the device ID.

**Modes**
Global configuration mode.

**Usage Guidelines**
The no form of this command disables truncating globally. Use the egress-truncate command to enable truncation. The egress-truncate-size command is supported globally for LAG ports.

**Examples**
The command must be enabled on a port or LAG using the egress-truncate command. The following example sets the size of the truncated egress packets to 200 bytes on all slots.

```
Brocade(config)#egress-truncate-size 200 slot all
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**email**

Configures the email ID for the Public Key Infrastructure (PKI) entity.

**Syntax**

```
email string
no email string
```

**Parameters**

*string*

Specifies the email ID for the PKI entity.

**Modes**

PKI entity configuration mode.

**Usage Guidelines**

The no form of the command removes the configured email ID.

**Examples**

The following example configures the email ID (user@brocade.com) for the PKI entity.

```
device(config)# pki entity test
device(config-pki-entity-test)# email user@brocade.com
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**enable-mka**

Enables MACsec Key Agreement (MKA) on a specified interface and changes the mode to dot1x-mka-interface mode to enable related parameters to be configured.

**Syntax**

```
enable-mka ethernet slot/port [to slot/port]
no enable-mka ethernet slot/port [to slot/port]
```

**Command Default**

MKA is not enabled on an interface.

**Parameters**

- **ethernet slot port**
  
  Specifies an Ethernet interface and the slot on the device, and the port on that slot.

**Modes**

- **dot1x-mka-interface mode**

**Usage Guidelines**

For a MACsec channel to be created between two ports, both ports and devices designated must have MACsec enabled and configured.

The **no** form of the command removes MACsec from the port.

**NOTE**

Primary port configuration will not be applied to all secondary ports in a LAG. LAG member ports should have individual configurations to enable MACsec.

**Examples**

The following example enables MACsec on Ethernet interface 1/1.

```
device(config-dot1x-mka)# enable-mka ethernet 1/1
device(config-dot1x-mka-eth-1/1)#
```

The following example configures MKA on multiple ports and enters the multiple interface configuration mode.

```
device(config-dot1x-mka)# enable-mka ethernet 1/1 to 1/10
device(config-dot1x-mka-mif-eth-1/1-1/10)#
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
enable-qos-statistics

Enables the collection of egress counter statistics on Brocade NetIron CER and CES series devices and enables the collection of
statistics for ingress and egress packet priorities on Brocade NetIron XMR and MLX series devices.

For Brocade NetIron XMR and MLX series devices the command has no parameters.

[no] enable-qos-statistics

Brocade NetIron CER and CES series devices only.
[no] enable-qos-statistics interface slot/port traffic-type { l2-l3 | vpls-vll-of } [ vlan vlan-id ] [ queue queue-num ] [ dp dp-value ]

Brocade NetIron CER and CES series devices.
no enable-qos-statistics interface slot/port [ traffic-type { l2-l3 | vpls-vll-of } [ vlan vlan-id ] [ queue queue-num ] [ dp dp-value ] ]

These parameters are for Brocade NetIron CER and CES series devices only.

interface slot/port

Enables counting of egress traffic on an interface identified by the slot on the device, and the port on that slot.

traffic-type

This keyword enables the counting of egress traffic that matches either physical Layer 2 and Layer 3 traffic or virtual VPLS/
VLL/ Openflow traffic.

l2-l3

This keyword specifies physical port traffic - Regular Layer 2 and Layer 3 egress traffic is counted.

vpls-vll-of

This keyword specifies that virtual port traffic - Virtual Private LAN Service (VPLS) or Virtual Leased Line (VLL) egress traffic is
counted.

vlan vlan-id

This option specifies that traffic that matches the VLAN ID is counted. The vlan-id ranges from 1 to 4090.

queue queue-num

This option specifies that traffic that matches the queue number is counted. The queue-num or traffic class ranges from 0 to 7.

dp dp-value

This option specifies that traffic that matches the drop precedence value is counted. The dp-value can be 0 to 3.

There are no command parameters for the Brocade NetIron XMR and MLX series devices.
The counters are disabled by default.

Global configuration mode.

For Brocade NetIron CER and CES series devices, the no form of the command can be used to disable egress counters at the interface
level.

For Brocade NetIron CER and CES series devices, only one egress statistics counter is supported per forwarding hardware.

For Brocade NetIron XMR and MLX series devices, the command has no parameters.

On Brocade NetIron CER and CES series devices, the following example enables all of the egress counters for regular Layer 2 and
Layer 3 traffic on interface 2/2.

device(config)# enable-qos-statistics interface 2/2 traffic-type l2-l3
On Brocade NetIron CER and CES series devices, the following example enables egress counters for regular Layer 2 and Layer 3 traffic on VLAN 200, queue 7, with a drop precedence value of 2.

```
    device(config)# enable-qos-statistics interface 2/1 traffic-type l2-l3 vlan 200 queue 7 dp 2
```

On Brocade NetIron CER and CES series devices, the following example disables egress counters at the interface level.

```
    device(config)# no enable-qos-statistics interface 2/1
```

On Brocade NetIron CER and CES series devices, the following example disables egress counters for regular Layer 2 and Layer 3 traffic on VLAN 200, queue 7, with a drop precedence value of 2.

```
    device(config)# no enable-qos-statistics interface 2/1 traffic-type l2-l3 vlan 200 queue 7 dp 2
```

On Brocade NetIron XMR and MLX series devices, the following command enables the collection of statistics for ingress and egress packet priorities.

```
    device(config)# enable-qos-statistics
    device(config)#
```

On Brocade NetIron XMR and MLX series devices, the following command disables the collection of statistics for ingress and egress packet priorities.

```
    device(config)# no enable-qos-statistics
    device(config)#
```

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00a</td>
<td>This command was modified to enable the collection of egress counter statistics on Brocade NetIron CER and CES series devices.</td>
</tr>
<tr>
<td>5.5.00</td>
<td>This command was introduced for Brocade NetIron XMR and MLX series devices.</td>
</tr>
</tbody>
</table>
**encapsulation-mode**

Specifies the encapsulation mode for an IPsec proposal.

**Syntax**

```
encapsulation-mode encapsulation-mode
```

**Command Default**

The default encapsulation mode is tunnel mode.

**Parameters**

```
encapsulation-mode
```

Specifies the encapsulation mode. Only tunnel mode is currently supported.

**Modes**

IPsec proposal configuration mode

**Usage Guidelines**

Because tunnel mode is configured by default and is the only mode that is currently supported, you do not need to configure the encapsulation mode for an IPsec proposal.

**Examples**

The following example shows how to configure tunnel mode as the encapsulation mode for an IPsec proposal named ipsec_proposal.

```
device(config)# ipsec proposal ipsec_proposal
device(config-ipsec-proposal-ipsec_proposal)# encapsulation-mode tunnel
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
encryption

Configures an encryption algorithm for an Internet Key Exchange version 2 (IKEv2) proposal.

Syntax

encryption { aes-cbc-128 | aes-cbc-256 }
no encryption { aes-cbc-128 | aes-cbc-256 }

Command Default

The default encryption algorithm is AES-CBC-256.

Parameters

- **aes-cbc-128**
  - Specifies the 128-bit advanced encryption standard algorithm in cipher block chaining mode.
- **aes-cbc-256**
  - Specifies the 256-bit advanced encryption standard algorithm in cipher block chaining mode.

Modes

IKEv2 proposal configuration mode

Usage Guidelines

The no form of the command removes the specified encryption algorithm configuration.

Examples

The following example shows how to configure the AES-CBC-128 encryption algorithm for an IKEv2 proposal named ikev2_proposal.

```plaintext
device(config)# ikev2 proposal ikev2_proposal
device(config-ikev2-proposal-ikev2_proposal)# encryption aes-cbc-128
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
enforce-first-as
Enforces the use of the first autonomous system (AS) path for external BGP (EBGP) routes.

Syntax

enforce-first-as
no enforce-first-as

Command Default
This option is disabled.

Modes
BGP configuration mode

Usage Guidelines
Use the no form of this command to restore the default.

This command causes the router to discard updates received from EBGP peers that do not list their AS number as the first AS path segment in the AS_PATH attribute of the incoming route.

Examples
This example configures the device to enforce the use of the first AS path.

device# configure terminal
device(config)# router bgp
device(config-bgp)# enforce-first-as
enrollment

Configures the enrollment information such as retry count, retry period, or profile for the polling interval for the certificate authority (CA).

Syntax

```
enrollment { retry-count count | retry-period period | profile profile name }
no enrollment { retry-count count | retry-period period | profile profile name }
```

Parameters

- **retry-count**
  - Specifies the retry count value to get the CA.
  - **count**
    - The retry count value in numbers. Valid numbers range from 1 through 100. The default is 10.

- **retry-period**
  - Specifies the time period to keep trying to get the CA.
  - **period**
    - The time period value in minutes. Valid numbers range from 1 through 60 minutes. The default is 1 minute.

- **profile**
  - Specifies the profile name to get the CA.
  - **profile name**
    - The profile name specified to get the CA.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The no form of the command disables the device from configuring enrollment options.

When the device configures the enrollment command for a second time to request the CA, the retry period between requests increases exponentially, with an additional 1 minute interval added at every increment.

Examples

The following example specifies the retry count value as 11.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# enrollment retry-count 11
```

The following example specifies the retry period of 2 minutes to get the CA.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# enrollment retry-period 2
```
The following example specifies the profile name as "Jane".

device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# enrollment Jane

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
esn-enable

Configures the Extended Sequence Number (ESN) for IPsec.

Syntax

```
esn-enable
no esn-enable
```

Command Default

Modes

IPsec proposal configuration mode.

Usage Guidelines

```
ipsec esn-enable
```

The `no` form of the command disables the ESN.

Examples

The following example configures the ESN for IPsec.

```
device(config)# ipsec proposal brocade
device(config-ipsec-proposal-brocade)# esn-enable
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**exclude-interface**

The user can create a bypass LSP by using the `bypass-lsp` command. The bypass LSP is the specification of excluded interfaces, which can be embodied as individual interfaces, ranges of interfaces, groups, or LAGs. Using this command the user can choose the interface to avoid as well as protect.

**Syntax**

```
exclude-interface { ethernet slot/port [ ethernet slot/port | to slot/port ] | pos slot/port [ pos slot/port | to slot/port ] | ve interface_id }
```

```
no exclude-interface { ethernet slot/port [ ethernet slot/port | to slot/port ] | pos slot/port [ pos slot/port | to slot/port ] | ve interface_id }
```

**Command Default**

By default, an interface is not protected.

**Parameters**

- **ethernet slot/port**
  - Specifies Ethernet port.

- **to slot/port**
  - Specifies the receiving port.

- **pos slot/port**
  - Specifies the selected individual POS interface port.

- **to slot/port**
  - Specifies the receiving port.

- **ve interface_id**
  - Specifies the selected Virtual Ethernet (VE) interface.

**Modes**

MPLS bypass LSP sub-configuration mode

**Usage Guidelines**

This is used for facility backup FRR. In the context of bypass LSP, the user can configure an MPLS interface as an exclude (protected) interface against resource failures using a bypass LSP. The user can specify a VE interface as exclude-interface. When a protected LSP egress interface is a VE interface, then any fault on a VE interface could trigger FastReroute. The following example configures protection for MPLS interface ve 100 using facility backup FRR.

The `no` form of the command removes the bypass LSP.
Examples

The following example displays the command.

device# configure terminal
device(config)# router-mpls
device(config-mpls)# bypass-lsp 123
device(config-mpls-bypass-lsp-123)# exclude-interface ethernet 1/1 ethernet 1/3
device(config-mpls-bypass-lsp-123)# exclude-interface ethernet 1/1 ethernet 1/3 to 1/4
**export-vrf-leaked-routes**

Redistributes routes imported from one VRF to another into VRF-BGP and advertises the route to the Layer 3 VPN network

**Syntax**

```
export-vrf-leaked-routes

no export-vrf-leaked-routes
```

**Command Default**

Enabled. Routes are not automatically blocked.

**Modes**

- Address family IPv4 VPN unicast configuration mode
- Address family IPv6 VPN unicast configuration mode

**Usage Guidelines**

The **no** form of the command blocks inter-VRF leaked routes.

The default behavior is backward compatible. A BGP option has been added to disable backward compatibility.

Starting in 5.8.00d and 5.9.00a, this command also disables inter-VRF-leaking of BGP routes with LSP next-hop.

**Examples**

This example blocks inter-VRF leaked routes from being advertised out to a Layer 3 VPN network for the IPv4 VPN unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family vpnv4 unicast
device(config-bgp-vpn4u)# no export-vrf-leaked-routes
```

This example blocks inter-VRF leaked routes from being advertised out to a Layer 3 VPN network for the IPv6 VPN unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family vpnv6 unicast
device(config-bgp-vpnv6)# no export-vrf-leaked-routes
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ni 5.6.00e</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.8.00d and 5.9.00a</td>
<td>This command was modified so that inter-VRF-leaking of BGP routes with LSP next-hop is disabled.</td>
</tr>
</tbody>
</table>
**external-lsdb-limit (OSPFv3)**

Configures the maximum size of the external link state database (LSDB).

**Syntax**

```
external-lsdb-limit value
no external-lsdb-limit
```

**Command Default**

250000

**Parameters**

`value`

Maximum size of the external LSDB. Valid values range from 1 through 250000.

**Modes**

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

**Usage Guidelines**

If you change the value, you must save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

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

**Examples**

The following example sets the limit of the external LSDB to 15000.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# external-lsdb-limit 15000
```
**ext-stats-mode slot**

Enables the extended statistics mode to display QinQ VLAN statistics.

**Syntax**

```
ext-stats-mode slot { number }
no ext-stats-mode slot { number }
```

**Command Default**

The extended statistics mode is not enabled.

**Parameters**

`number`

Specifies the interface module slot number for a 32-slot chassis (1-32), a 16-slot chassis (1-16), an 8-slot chassis (1-8), and a 4-slot chassis (1-4).

**Modes**

Global configuration mode

**Usage Guidelines**

Use this command to enable egress QinQ statistics when the extended counters are configured for a particular VPLS, VLL, or VLL-local instance. Extended statistics is enabled for ingress QinQ statistics by default. This CLI is added to support egress QinQ statistics. The QinQ statistics support is enabled only for QinQ VLANs configured under VPLS, VLL, and VLL-local.

This command configuration is supported on the Brocade MLX Series and Brocade NetIron XMR Series devices. On the BR-MLX-10Gx24 interface module, only the ingress QinQ statistics extended counters are supported. Gen1.1 modules are not supported.

When the command is enabled, the number of counters supported for egress port VLAN statistics per NP is reduced to 8191. There is no change to the number of counters for ingress. When the command is not enabled for QinQ statistics, the number of counters supported for ingress and egress does not change. The following table details the number of egress port VLAN counters supported on both ingress and egress counters, before and after enabling the `ext-stats-mode slot` command.

<table>
<thead>
<tr>
<th>Switched and routed packets</th>
<th>Account based on internal priority of packet</th>
<th>Number of unique egress port-VLAN that have counters (pre-5.9)</th>
<th>Number of unique egress port-VLAN counters after enabling QinQ statistics mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch and Route combined</td>
<td>No</td>
<td>32767 on ingress and 32767 on egress; each set having 8 counters.</td>
<td>32767 on ingress and 8191 on egress; each set having 1 counter.</td>
</tr>
<tr>
<td>Switch and Route combined</td>
<td>Yes</td>
<td>4095 on ingress and 4095 on egress; each set having 8 counters.</td>
<td>4095 on ingress and 4095 on egress; each set having 8 counters.</td>
</tr>
<tr>
<td>Switch or Route separately</td>
<td>No</td>
<td>16383 on ingress and 16383 on egress; each set having 2 counters.</td>
<td>16383 on ingress and 8191 on egress; each set having 2 counters.</td>
</tr>
</tbody>
</table>
Switched and routed packets | Account based on internal priority of packet | Number of unique egress port-VLAN that have counters (pre-5.9) | Number of unique egress port-VLAN counters after enabling QinQ statistics mode
---|---|---|---
Switch or Route separately | Yes | 2047 on ingress and 2047 on egress; each set having 16 counters. | 2047 on ingress and 2047 on egress; each set having 16 counters.

You must reload the interface module for the command to go into effect. A warning message of the required reload is displayed when the command is executed.

A syslog and warning message is generated if all 8191 egress statistics are utilized on a specific LP. A warning message similar to the following is displayed:

`Warning: Extended-Counter Egress Stats ID allocation failed for VPLS Eth 2/1 Vlan Id 200, Inner Vlan Id 500`

There is a set number of counters supported per NP from hardware. If you receive this message, you can move the ports to the other NP. Each vport (port-VLAN combination) utilizes one statistics ID.

The `show mpls statistics vpls` and `clear mpls statistics vpls` commands are modified to include the parameter `inner-vlan vlan-id`. The parameter specifies the ID of the configured inner VLAN. If the `inner-vlan vlan-id` parameter is not specified, the output displays vlan statistics only. To display specific tx/egress statistics, the `ext-stats-mode` command must be enabled for the LP module. If the command is not enabled for a specific slot, the QinQ statistics displays an NA value for ports of that slot.

The `no` form of the command disables the extended statistics mode to display QinQ VLAN statistics.

**Examples**

The following example enables the extended statistics mode to display QinQ VLAN statistics on interface module slot 4.

```
device(config)# ext-stats-mode slot 4
Please write memory. LP-2 reload is required for ext-stats-mode enable/disable to take effect.
```

Use the `show running-config` command to display the configuration for the `ext-stats-mode` command.

```
device(config)# show running-config | inc ext-stats-mode
ext-stats-mode slot 1
ext-stats-mode slot 2
ext-stats-mode slot 3
ext-stats-mode slot 4
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Commands F - J**

**fast-external-fallover**

Resets the session if a link to an eBGP peer goes down.

**Syntax**

- `fast-external-fallover`
- `no fast-external-fallover`

**Command Default**

This option is disabled.

**Modes**

- BGP configuration mode

**Usage Guidelines**

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

Use this command to terminate and reset external BGP sessions of a directly adjacent peer if the link to the peer goes down, without waiting for the timer, set by the BGP `timers` command, to expire. This can improve BGP conversion time, but can also lead to instability in the BGP routing table as a result of a flapping interface.

**Examples**

This example configures the device to reset the session if a link to an eBGP peer goes down.

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

```
device(config-bgp)# fast-external-fallover
```
fingerprint

Configures the fingerprint for the Certificate Authority (CA).

Syntax

fingerprint hex-data

Parameters

hex-data

Specifies the hex data for the fingerprint in the xxx:xxx:xx format.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

When the CA sends the certificate, it should match the fingerprint configured for the certificate to be accepted.

Examples

The following example configures the fingerprint for the CA.

device(config)# pki-trustpoint test
93:74:c3

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
fqdn

Configures the fully qualified domain name (FQDN) for the PKI entity.

Syntax

fqdn string

Parameters

string

Specifies the FQDN for PKI entity.

Modes

PKI entity configuration mode.

Examples

The following example configures the FQDN for the PKI entity.

device(config)# pki entity brocade_entity
device(config-pki-entity-brocade_entity)# fqdn red

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
garp-ra-interval

Sets the interval between gratuitous ARP (GARP) router advertisements when Virtual Router Redundancy Protocol Extended (VRRP-E) scaling is configured.

Syntax

```
garp-ra-interval interval
no garp-ra-interval interval
```

Command Default

Gratuitous ARP router advertisements are sent every 30 seconds.

Parameters

```
interval
```

Sets the gratuitous ARP router advertisements interval timer, in seconds. Values range from 30 to 120 seconds. Default is 30 seconds.

Modes

Global configuration mode

Usage Guidelines

This command is used with the VRRP-E scaling feature where VRRP-E instances are grouped and hello messages between group members are stopped to reduce the CPU load and allow more VRRP-E instances to be configured. Gratuitous ARP messages are still sent by the group master on behalf of its members to advertise the virtual MAC address to devices on the network, but at a longer intervals.

The `no` form of this command resets the default value of 30 seconds between gratuitous ARP router advertisements.

Examples

The following example sets the gratuitous ARP router advertisement interval to 90 seconds.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# garp-ra-interval 90
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
gig-default

Enables auto-negotiation support for 1G ports.

Syntax

gig-default { auto-gig | neg-off | auto-full | neg-full-auto }

no gig-default { auto-gig | neg-off | auto-full | neg-full-auto }

Command Default

The default value is auto.

Parameters

auto-gig

The port tries to perform a negotiation with its peer port to exchange capability information. This is the default state.

neg-off

The port does not try to perform a negotiation with its peer port.

auto-full

The port tries to perform a negotiation with its peer port to exchange capability information. If it is unable to reach an agreed upon speed, the port goes into a fixed speed and keeps the link up.

neg-full-auto

The port is only for copper-SFP and to support 10/100/1000M tri-speed auto negotiation.

Modes

EXEC mode.

Usage Guidelines

Unless the ports at both ends of a Gigabit Ethernet link use the same mode (either auto-gig or neg-off), the ports cannot establish a link. An administrator must intervene to manually configure one or both sides of the link to enable the ports to establish the link.

The no form of the command disables Remote Fault Notification (RFN) after enabling.

Supports the following modules:

- 20x10GE
- 4x10GE-IPSEC

Examples

The following example displays how to change the negotiation mode for individual port.

device(config)# interface ethernet 4/1 to 4/4
device(config-mif-4/1-4/4)# gig-default neg-off
### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00a</td>
<td>This command was modified include the parameters <code>neg-off</code> and <code>auto</code>.</td>
</tr>
</tbody>
</table>
**graceful-restart (OSPFv2)**

Enables the OSPF Graceful Restart (GR) capability.

**Syntax**

```
graceful-restart [ helper-disable | restart-time seconds ]
no graceful-restart
```

**Command Default**

Graceful restart and graceful restart helper capabilities are enabled.

**Parameters**

- `helper-disable`
  Disables the GR helper capability.

- `restart-time`
  Specifies the maximum restart wait time, in seconds, advertised to neighbors. The default value is 120 seconds. The configurable range of values is from 10 through 1800 seconds.

**Modes**

- OSPF router configuration mode
- OSPF router VRF configuration mode

**Usage Guidelines**

Use `no graceful-restart helper-disable` to re-enable the GR helper capability.

The `no` form of the command disables the graceful restart capability.

**Examples**

The following example disables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# graceful-restart helper-disable
```

The following example re-enables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# no graceful-restart helper-disable
```

The following example re-enables the GR capability.

```
device# configure terminal
device(config)# rbridge-id 10
device(config-rbridge-id-10)# router ospf
device(config-router-ospf-vrf-default-vrf)# graceful-restart
```
The following example re-enables the GR capability and changes the maximum restart wait time from the default value to 240 seconds.

device# configure terminal
device(config)# router ospf
device(config-ospf-router)# graceful-restart restart-time 240
graceful-restart helper (OSPFv3)

Enables the OSPFv3 graceful restart (GR) helper capability.

Syntax

graceful-restart helper { disable | strict-lsa-checking }
no graceful-restart helper

Command Default

GR helper is enabled.

Parameters

disable

Disables the OSPFv3 GR helper capability.

strict-lsa-checking

Enables the OSPFv3 GR helper mode with strict link-state advertisement (LSA) checking.

Modes

OSPFv3 router configuration mode
OSPFv3 router VRF configuration mode

Usage Guidelines

The no form of the command disables the GR helper capability on a device.

Examples

The following example enables GR helper and sets strict LSA checking.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router-ospf)# graceful-restart helper strict-lsa-checking
group-master interface

Configures a Virtual Router Redundancy Protocol Extended (VRRP-E) device in interface configuration mode as the VRRP-E group master of a logical grouping of VRRP-E instances.

Syntax

```
group-master interface { ethernet slot/port | ve vrid } vrid id
no group-master interface { ethernet slot/port | ve vrid } vrid id
```

Command Default

No group master is configured.

Parameters

- **ethernet slot/port**
  
  Configures the VRRP-E group master for the specified port.

- **ve vrid**
  
  Configures the VRRP-E group master for the specified virtual Ethernet port.

- **vrid id**
  
  Assigns the VRID of the group master for the specified port.

Modes

Virtual router interface configuration mode

Usage Guidelines

This command is used as a grouping mechanism to allow the scaling of the number of VRRP extended (VRRP-E) instances up to 4000 instances. VRRP-E instances are configured into logical groups consistently across all the VRRP-E master and backup devices.

The `no` form of this command removes the grouping configuration.

Examples

The following examples configures virtual router 1 on interface ve 1 as the VRRP-E group master of the virtual router 2 on interface ve 2.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ve 2
device(config-vif-2)# ip address 10.53.5.1/24
device(config-vif-2)# ip vrrp vrid 2
device(config-vif-2-vrid-2)# group-master interface ve 1 vrid 1
```
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**hello-interval (VRRP)**

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

**Syntax**

```
hello-interval [ msec ] interval
no hello-interval [ msec ] interval
```

**Command Default**

Hello messages from VRRP master routers are sent to backup routers every second.

**Parameters**

- `msec interval`
  - Interval, in milliseconds, at which a master VRRP router advertises its existence to the backup VRRP routers. Valid values range from 100 through 84000. The default is 1000. VRRP-E does not support the hello message interval in milliseconds.

- `interval`
  - Sets the interval, in seconds, for which a VRRP backup router waits for a hello message from the VRRP master router before determining that the master is offline. Valid values range from 1 through 84. The default value is 1.

**Modes**

VRID interface configuration mode

**Usage Guidelines**

A VRRP master router periodically sends hello messages to the backup routers. The backup routers use the hello messages as verification that the master is still online. If the backup routers stop receiving the hello messages for the period of time specified by the dead interval, the backup routers determine that the master router is dead. At that point, the backup router with the highest priority becomes the new master router.

By default, the dead interval is internally derived from the hello interval. It is equal to 3 times the hello interval plus the skew time, where the skew time is equal to (256 minus the priority) divided by 256. Generally, if you change the hello interval on the master VRRP router using the `hello-interval` command, you also should also change the dead interval on the VRRP backup routers using the `dead-interval` command.

The `hello-interval` command is configured only on master VRRP routers and is supported by VRRP and VRRP-E.

The `no` form resets the hello message interval to its default value of 1000 milliseconds (1 second).

**NOTE**

VRRP-E does not support the hello message interval in milliseconds.
Examples

The following example enables advertisements from the VRRP master router and sets the hello message interval to 10,000 milliseconds.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# hello-interval msec 10000
device(config-if-e1000-1/6-vrid-1)# activate
```

The following example enables advertisements from the VRRP-E master router and sets the hello message interval to 15 seconds.

```
device# configure terminal
device(config)# router vrrp-extended
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.3/24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 50 track-priority 10
device(config-if-e1000-1/5-vrid-2)# ip-address 10.53.5.1
device(config-if-e1000-1/5-vrid-2)# hello-interval 15
device(config-if-e1000-1/5-vrid-2)# activate
```
**hello-time**

Sets the hello time value for metro ring packets.

**Syntax**

```
hello-time ms
no hello-time ms
```

**Command Default**

The hello time value is not preset.

**Parameters**

- `ms`

The hello time value that is entered as multiples of 100 milliseconds. The valid values are 100 through 15000 entered as multiples of 100 ms. For example, a valid multiple of 100 ms can be 200, 700, 1300, 14000, and so on. Invalid value of 100 ms can be 221, 740, 1228, 1445, and so on. The default value is 100 ms.

**Modes**

- MRP configuration mode

**Usage Guidelines**

The `no` form of the command resets the hello time that was defined for the hello ring packets.

**Examples**

The following example sets a value of 400 ms for the ring packets.

```
device(config)# vlan 1
device(config-vlan-1)# metro-ring 1
device(config-vlan-1-mrp-1)# hello-time 400
```
ike-profile

Configures the IKE profile attached with the IPsec profile.

Syntax
ike-profile ike-profile-name
no ike-profile ike-profile-name

Parameters
ike-profile-name
Specifies the IKE profile name attached with the IPsec profile.

Modes
IPsec profile configuration mode

Usage Guidelines
no

Examples
The following example configures the IKE profile attached with IPsec profile.

device(config)# ipsec profile brocade
device(config-ipsec-profile-brocade)# ike-profile red

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 auth-proposal

Creates an Internet Key Exchange version 2 (IKEv2) authentication proposal and enters configuration mode for the proposal.

Syntax

ikev2 auth-proposal auth-name
no ikev2 auth-proposal auth-name

Parameters

auth-name

Specifies the name of an IKEv2 authentication proposal.

Modes

Global configuration mode

Usage Guidelines

An IKEv2 authentication proposal defines the authentication methods used in IKEv2 peer negotiations.

An IKEv2 authentication proposal is activated by attaching it to an IKEv2 profile.

The no form of the command removes the IKEv2 authentication proposal configuration.

Examples

The following example shows how to create an IKEv2 authentication proposal named "secure" and enters configuration mode for the proposal.

device# configure terminal
device(config)# ikev2 auth-proposal secure
device(config-ike-auth-proposal-secure)#

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 cookie-challenge

Enables the Internet Key Exchange version 2 (IKEv2) cookie challenge option.

Syntax

```
cookie-challenge number
no cookie-challenge number
```

Command Default

By default, this command is disabled.

Parameters

```
number
```

Specifies the maximum number of Security Associations (SA) supported. The maximum number of SAs supported are from 1 through 2000.

Modes

Global configuration mode.

Usage Guidelines

The command is enabled only when the maximum number of half-open IKE SAs go beyond the configured cookie challenge number.

The no form of the command disables the cookie challenge number.

Examples

The following example configures an IKEv2 cookie challenge.

```
device(config)# ikev2 cookie-challenge 5
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 dhgroup

Configures the group used for Diffie-Hellman (DH) negotiations.

Syntax

ikev2 dhgroup { 1 } { 2 } { 5 } { 14 } { 15 } { 16 } { 19 } { 20 } { 24 }

Parameters

1  Specifies the 768-bit DH group.
2  Specifies the 1024-bit DH group.
5  Specifies the 1536-bit DH group.
14 Specifies the 2048-bit DH group.
15 Specifies the 3072-bit DH group.
16 Specifies the 4096-bit DH group.
19 Specifies the 256-bit elliptic curve DH (ECDH) group.
20 Specifies the 384-bit ECDH group.
24 Specifies the 2048-bit DH/SA group.

Modes

IKEv2 proposal configuration mode.

Examples

The following example configures the group used for Diffie-Hellman (DH) negotiations.

device(config)# ikev2-proposal
device(config-ikev2-proposal)# ikev2 dhgroup 20

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 exchange-max-time

Configures the maximum setup time for Internet Key Exchange version 2 (IKEv2) message exchange.

Syntax

```plaintext
ikev2 exchange-max-time seconds
no ikev2 exchange-max-time seconds
```

Command Default

The default value is 30 seconds.

Parameters

```plaintext
seconds
```

Specifies the maximum setup time in seconds. The time range is from 1 through 300 seconds.

Modes

Global configuration mode.

Usage Guidelines

The no form of the command resets the maximum setup time to the default value.

Examples

The following example sets the maximum setup time for IKEv2 message exchange to 50 seconds.

```plaintext
device# configure terminal
device(config)# ikev2 exchange-max-time 50
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 http-url-cert

Configures the HTTP certification support.

Syntax

ikev2 http-url-cert
no ikev2 http-url-cert

Command Default

By default, this command is disabled.

Modes

Global configuration mode.

Usage Guidelines

The no form of the command removes the configured HTTP certification support.

Examples

The following example configures HTTP certification support.

device(config)# ikev2 http-url-cert

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 limit

Configures limits for the number of Internet Key Exchange version 2 (IKEv2) security association (SA) sessions.

Syntax

ikev2 limit { max-in-negotiation-sa limit | max-sa limit limit }
no ikev2 limit { max-in-negotiation-sa limit | max-sa limit limit }

Command Default

The default limit (for each type of SA session) is 256.

Parameters

max-in-negotiation-sa limit

Limits the total number of in-negotiation IKEv2 SA sessions. The range is from 1 through 256.

max-sa limit

Limits the total number of IKEv2 SA sessions. The range is from 1 through 256.

Modes

Global configuration mode

Usage Guidelines

The no form of the command returns the specified SA session limit to the default value.

Examples

The following example shows how to limit the maximum number of in-negotiation IKEv2 SA sessions to 10.

device# configure terminal
device(config)# ikev2 limit max-in-negotiation-sa 10

The following example shows how to limit the maximum number of IKEv2 SA sessions to 200.

device# configure terminal
device(config)# ikev2 limit max-sa 200

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 nat-enable

Globally enables IP security (IPsec) over Network Address Translation (NAT).

Syntax

ikev2 nat-enable
no ikev2 nat-enable

Command Default

IPsec over NAT is disabled.

Modes

Global configuration mode

Usage Guidelines

Before configuring this command, ensure that a NAT device is located between two Internet Key Exchange (IKE) peers or one of the IKE peers must support NAT functionality to address the change of the IP/TCP header in packets. When IPsec over NAT is enabled, the negotiation of NAT Traversal (NAT-T) between the IKE peers is started and if the negotiation is successful, all encapsulating security payload (ESP) packets sent over the tunnel are encapsulated in the UDP header.

The no form of this command disables the IPsec tunnels and the IKE exchange is renegotiated without NAT-T.

NOTE

The ikev2 nat-enable command is supported only by Brocade MLXe Series devices.

Examples

The following example globally enables IPsec over NAT.

device# configure terminal
device(config)# ikev2 nat-enable

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 nat-keepalive

Configures a time interval during which NAT keep-alive messages are sent when the IP security (IPsec) over Network Address Translation (NAT) feature is enabled.

Syntax

ikev2 nat-keepalive [ time ]
no ikev2 nat-keepalive [ time ]

Command Default

The default is 20 seconds.

Parameters

  time

  Time interval, in seconds, during which NAT keep-alive messages are sent.

Modes

  Global configuration mode

Usage Guidelines

This command is used in conjunction with the ikev2 nat-enable command that enables IPsec over NAT. The keepalive messages are sent periodically to keep the NAT mappings running.

The no form of this command resets the keepalive interval to 20 seconds.

NOTE

The ikev2 nat-keepalive command is supported only by Brocade MLXe Series devices.

Examples

The following example globally enables IPsec over NAT and sets the keepalive interval to 10 seconds.

  device# configure terminal
device(config)# ikev2 nat-enable
device(config)# ikev2 nat-keepalive 10

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 policy

Creates an Internet Key Exchange version 2 (IKEv2) policy and enters IKEv2 policy configuration mode.

Syntax

ikev2 policy name

no ikev2 policy name

Command Default

The default IKEv2 policy is def-ike-policy.

Parameters

name

Specifies the name of an IKEv2 policy.

Modes

Global configuration mode

Usage Guidelines

Use the ikev2 policy command to configure any additional IKEv2 policies that you need.

The no form of the command removes any IKEv2 policy configuration other than the default IKEv2 policy.

The default IKEv2 policy cannot be removed.

Only one IKEv2 policy can be selected for a local endpoint (single IPv4 or IPv6 address). Multiple IKEv2 policies selected for the same IP address is invalid.

When multiple matching policies are identified during IKEv2 negotiations, the most recently created matching policy is used.

Examples

The following example creates an IKEv2 policy named test_policy1.

device# configure terminal
device(config)# ikev2 policy test_policy1
device(config-ike-policy-test_policy1)#

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 profile

Configures the specified IKEv2 profile and gives you the option of identifying the local endpoint of the tunnel. This command supports IPsec IPv4 and IPv6.

Syntax

```
ikev2 profile { name[local-identifier]{address [ipv4-address |ipv6-address] | [dndn-string] | [fqdnfqdn-string] | [key-idkey-id string] | [emailemail-string] | [remote-identifier]{address [ipv4-address |ipv6-address] | [dndn-string] | [fqdnfqdn-string] | [key-idkey-id string] | [emailemail-string]}

match identitylocaladdress

no ikev2 profile { name[local-identifier]{address [ipv4-address |ipv6-address] | [dndn-string] | [fqdnfqdn-string] | [key-idkey-id string] | [emailemail-string] | [remote-identifier]{address [ipv4-address |ipv6-address] | [dndn-string] | [fqdnfqdn-string] | [key-idkey-id string] | [emailemail-string]}
```

Command Default

This command is not configured.

Parameters

- **name**
  Specifies the IKEv2 profile name.

- **local-identifier**
  (Optional) Identifies the local endpoint of the tunnel. You can identify the endpoint using the IP address, distinguished name (dn), fully qualified domain name (fqdn), key identifier (key-id), or email.

  - **address [ipv4-address |ipv6-address]**
    Identifies the local endpoint of the tunnel using the IPv4 or IPv6 IP address.

  - **dn string**
    Identifies the local endpoint of the tunnel using the LDAP distinguished name.

  - **fqdn string**
    Identifies the local endpoint of the tunnel using the fully qualified domain name.

  - **key-id string**
    Identifies the local endpoint of the tunnel using the key identifier (ID).

  - **email string**
    Identifies the local endpoint of the tunnel using the email address.

- **remote-identifier**
  (Optional) Identifies the remote endpoint of the tunnel. You can identify the endpoint using the IP address, distinguished name (dn), fully qualified domain name (fqdn), key identifier (key-id), or email.

  - **address [ipv4-address |ipv6-address]**
    Identifies the remote endpoint of the tunnel using the IPv4 or IPv6 IP address.

  - **dn string**
    Identifies the remote endpoint of the tunnel using the LDAP distinguished name.
fqdn\text{string}
Identifies the remote endpoint of the tunnel using the fully qualified domain name.

key-id\text{string}
Identifies the remote endpoint of the tunnel using the key identifier (ID).

e-mail\text{string}
Identifies the remote endpoint of the tunnel using the email address.

match identity
(Optional) Causes the IKE profile Peer Authorization Database (PAD) for the peers to be automatically selected based on the identity parameters received by the local or remote endpoints. The parameters you specify are used to select the PAD.

**Modes**
Global configuration mode.

**Usage Guidelines**
no

Using the command automatically enters IKEv2 profile configuration mode.

**Examples**
The following example configures the IKEv2 profile named test1.

device(config)# ikev2 profile test1
Need example showing new parameters.

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to add support for IPsec IPv6 and to add the local identifier option.</td>
</tr>
</tbody>
</table>
ikev2 proposal

Creates an Internet Key Exchange version 2 (IKEv2) proposal and enters IKEv2 proposal configuration mode.

Syntax

ikev2 proposal name
no ikev2 proposal name

Command Default

The default IKEv2 proposal is \texttt{def-ike-proposal}.

Parameters

name

Specifies the name of an IKEv2 proposal.

Modes

Global configuration mode

Usage Guidelines

An IKEv2 proposal defines a set of algorithms that are used in IKEv2 peer negotiations.

The \texttt{no} form of the command removes any IKEv2 proposal configuration other than the default IKEv2 proposal configuration.

Examples

The following example shows how to create an IKEv2 proposal named test_proposal1.

device# configure terminal
device(config)# ikev2 proposal test_proposal1
device(config-ike-proposal-test_proposal1)#

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 retransmit-interval
ConFigures the delay time for resending Internet Key Exchange version 2 (IKEv2) messages.

Syntax
ikev2 retransmit-interval time
no ikev2 retransmit-interval time

Command Default
The default delay time is 5 seconds.

Parameters
time
Specifies the delay time in seconds. The time ranges from 1 through 60.

Modes
Global configuration mode

Usage Guidelines
The retransmit interval increases exponentially.
The no form of the command restores the default value.

Examples
The following example show how to configure the delay time for resending IKEv2 messages to 20 seconds.

device# configure terminal
device(config)# ikev2 retransmit-interval 20

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ikev2 retry-count

Configures the maximum number of attempts to retransmit an Internet Key Exchange version 2 (IKEv2) message.

Syntax

ikev2 retry-count number
no ikev2 retry-count number

Command Default

The default number of attempts is 5.

Parameters

number

Specifies the maximum number of attempts to retransmit an IKE message. The range is from 1 through 25.

Modes

Global configuration mode

Usage Guidelines

The no form of the command resets the retry count to the default value.

Examples

The following example shows how to configure the number of retry attempts for transmitting an IKEv2 message to 8.

device# configure terminal
device(config)# ikev2 retry-count 8

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ike-profile

Configures the IKE profile attached with the IPsec profile.

Syntax

ike-profile ike-profile-name
no ike-profile ike-profile-name

Parameters

ike-profile-name

Specifies the IKE profile name attached with the IPsec profile.

Modes

IPsec profile configuration mode

Usage Guidelines

no

Examples

The following example configures the IKE profile attached with IPsec profile.

device(config)# ipsec profile brocade
device(config-ipsec-profile-brocade)# ike-profile red

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**ingress-tunnel-accounting**

Excludes the Ethernet header (14 bytes) and Ethernet overhead (20 bytes) and CRC overhead (four bytes) when collecting byte statistics. In other words, it counts only the size of the MPLS packet.

**Syntax**

```
ingress-tunnel-accounting exclude-ethernet-overhead
no ingress-tunnel-accounting exclude-ethernet-overhead
```

**Command Default**

None.

**Modes**

MPLS policy configuration mode

**Usage Guidelines**

The operation of the command, based on the operator input, can be defined as ‘y’ – the configuration change is done and the counters are cleared, or ‘n’ – the configuration change is not done and the counters are not cleared.

The command `no ingress-tunnel-accounting exclude-ethernet-overhead` disables only the exclude-ethernet-overhead option.

To disable ingress-tunnel-accounting itself, enter the command `no ingress-tunnel-accounting`.

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to enforce the clearing of counters when <code>exclude-ethernet-overhead</code> mode is changed, a confirmation message is added to the command and on execution, the command clears the counters.</td>
</tr>
<tr>
<td>5.6.00</td>
<td>This command modified the <code>exclude-ethernet-overhead</code> option, lets the operator exclude the Ethernet header and Ethernet overhead and CRC overhead when collecting the byte statistics.</td>
</tr>
</tbody>
</table>
In-label

Specifies the label that is received in the packets and used to identify the static transit LSP in the router. This, in turn, decides where the next hop will be based on the "next-hop" configuration.

Syntax

in-label value

no in-label value

Parameters

value

Represents the label received in the MPLS header in the packets from upstream. Acceptable ranges for the parameter include Static label min-value and Static label max-value. The value must not exceed the static label range configured on the router.

Modes

MPLS-transit LSP sub-configuration mode.

Usage Guidelines

Examples

The following example displays the in-label command:

device# configure terminal
device(config)# router mpls
device(config-mpls)# static-transit t1
device(config-mpls-static-transit-t1)# in-label 16
install-igp-cost
Configures the device to use the IGP cost instead of the default BGP Multi-Exit Discriminator (MED) value as the route cost when the route is added to the Routing Table Manager (RTM).

Syntax
install-igp-cost
no install-igp-cost

Command Default
This option is disabled.

Modes
BGP configuration mode

Usage Guidelines
By default, BGP uses the BGP MED value as the route cost when the route is added to the RTM. Use this command to change the default to the IGP cost.

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

Examples
This example configures the device to compare MEDs.

device# configure terminal
device(config)# router bgp
device(config-bgp)# install-igp-cost
integrity

Configures an integrity algorithm for an Internet Key Exchange version 2 (IKEv2) proposal.

Syntax

```
integrity { sha256 | sha384 }
no integrity { sha256 | sha384 }
```

Command Default

The default integrity algorithm is SHA-384.

Parameters

- `sha256`
  Specifies SHA-2 family 256-bit (hash message authentication code (HMAC) variant) as the hash algorithm.

- `sha384`
  Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.

Modes

IKEv2 proposal configuration mode

Usage Guidelines

Multiple integrity algorithms may be configured for an IKEv2 proposal.

When only one integrity algorithm is configured for an IKEv2 proposal, removing it restores the default configuration.

The `no` form of the command removes the specified integrity algorithm configuration.

Examples

The following example shows how to configure the integrity algorithm SHA-256 for an IKEv2 proposal name ikev2_proposal.

```
device(config)# ikev2 proposal ikev2_proposal
device(config-ikev2-proposal-ikev2_proposal)# integrity sha256
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip

Configures the IP address used in the certificate for the PKI entity.

Syntax

   ip ip-address
   no ip ip-address

Parameters

   ip-address
     Specifies the IP address for the PKI entity.

Modes

   PKI entity configuration mode.

Usage Guidelines

   no

Examples

   The following example configures the IP address for the PKI entity.

   device(config)# pki entity brocade
   device(config-pki-entity-brocade)# ip 10.10.20.1

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**ip access-group**

Applies rules specified in an IPv4 access control list (ACL) to traffic entering or exiting an interface.

**Syntax**

```
ip access-group { acl-num | acl-name } { in | out }
no ip access-group { acl-num | acl-name } { in | out }
```

```
ip access-group { acl-num | acl-name } in [ ethernet slot / port ... ] [ ethernet slot / port to ethernet slot / port ... ]
no ip access-group { acl-num | acl-name } in [ ethernet slot / port ... ] [ ethernet slot / port to ethernet slot / port ... ]
```

**Command Default**

ACLs are not applied to interfaces.

**Parameters**

- **acl-num**
  Specifies an ACL number. You can specify from 1 through 99 for standard ACLs and from 100 through 199 for extended ACLs.

- **acl-name**
  Specifies a valid ACL name.

- **in**
  Applies the ACL to inbound traffic on the port.

- **ethernet slot / port**
  Specifies the Ethernet interface from which the packets are coming.

- **to slot / port**
  Specifies the range of Ethernet interfaces from which the packets are coming.

- **out**
  Applies the ACL to outbound traffic on the port.

**Modes**

Interface subtype configuration modes

**Usage Guidelines**

To apply an IPv4 ACL name that contains spaces, enclose the name in quotation marks (for example, `ip access-group standard "ACL for Net1" in`).

Through a virtual routing interface, you have the following options:

- (Default) Apply an ACL to all ports of the VLAN.
- One or both of the following options:
  - Apply an ACL to specified ports.
- Apply an ACL to one or more ranges of ports.

To remove an ACL from an interface, use one of the `no` forms of this command.

**Examples**

The following example creates a named standard IPv4 ACL, defines rules in the ACL, and applies it on an ethernet interface in the ingress direction:

```
device# configure terminal
device(config)# ip access-list standard Net1
device(config-std-nacl-Net1)# deny host 10.157.22.26
device(config-std-nacl-Net1)# deny 10.157.29.12
device(config-std-nacl-Net1)# deny host IPHost1
device(config-std-nacl-Net1)# permit any
device(config-std-nacl-Net1)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group Net1 in
```

The following example creates a named extended IPv4 ACL, defines rules in the ACL, and applies it on an ethernet interface in the ingress direction:

```
device# configure terminal
device(config)# ip access-list extended "block Telnet"
device(config-ext-nacl-block telnet)# deny tcp host 10.157.22.26 any eq telnet
device(config-ext-nacl-block telnet)# permit ip any any
device(config-ext-nacl-block telnet)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group "block Telnet" in
```

The following example configures port-based VLAN 10, adds ports 1/1 through 2/12 to the VLAN, and then adds virtual routing interface 1 to the VLAN.

```
The commands following the first line-break configure a standard numbered IPv4 ACL, using the `access-list` command. (You can also use the `ip access list { standard | extended }` command.)

The commands following the second line-break apply the ACL, in an ingress direction, to a subset of the ports associated with virtual interface 1 and to outgoing traffic on all ports.

```
device# configure terminal
device(config)# vlan 10 name IP-subnet-vlan
device(config-vlan-10)# untag ethernet 1/1 to 1/20 ethernet 2/1 to 2/12
device(config-vlan-10)# router-interface ve 1
device(config-vlan-10)# exit

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

device(config)# interface ve 1
device(config-vif-1)# ip access-group 1 in ethernet 1/1 ethernet 1/3 ethernet 2/1 to 2/4
device(config-vif-1)# ip access-group 1 out
```
**ip access-group enable-deny-logging**

Running this command on an interface is one of the conditions for enabling logging of traffic denied by IPv4 ACLs applied to the interface. The other condition is the inclusion of the log parameter in rules within such ACLs.

**Syntax**

```
ip access-group enable-deny-logging [ hw-drop ]
no ip access-group enable-deny-logging [ hw-drop ]
```

**Command Default**

Deny-logging for IPv4 ACLs is disabled.

**Parameters**

- **hw-drop**
  Specifies that IPv4 ACL-log packets be dropped in hardware, which reduces CPU load.

**Modes**

Interface subtype configuration modes

**Usage Guidelines**

When this command is implemented with the *hw-drop* option, packet-counts of denied traffic will include only the first packet in each time cycle.

Deny-logging is supported for inbound ACLs only.

Deny-logging generates Syslog entries only. No SNMP traps are issued.

VPLS, VLL, and VLL-local endpoints do not support the *ip access-group enable-deny-logging* command.

On Brocade NetIron CES Series and Brocade NetIron CER Series devices, deny-logging takes precedence over ACL accounting. If the *ip access-group enable-deny-logging* command is configured on an interface, and both *enable-accounting* and *log* are present in an ACL rule, statistics for that rule are not collected. The output of the *show access-list accounting* command will indicate that logging is enabled, and that statistics for that ACL rule are not available.

This command is not needed on management interfaces, which log both *permit* and *deny* rules that contain a *log* keyword.

Implementation of both deny-logging and denied-traffic redirection (*ip access-group redirect-deny-to-interf*) on an interface can affect denied-traffic forwarding. For rules that contain the log keyword, deny-logging prevents denied-traffic redirection.

To disable IPv4 ACL deny-logging on an interface, use the `no ip access-group enable-deny-logging` command. You do not have to remove log parameters from ACLs and re-apply the ACLs.

To disable the *hw-drop* option, use the `no ip access-group enable-deny-logging hw-drop` command.
### Examples

The following example implements IPv4 ACL deny-logging on an interface—for applied ACLs that contain rules with `log` parameters.

```
device# configure terminal
device(config)# interface ethernet 5/1
device(config-if-e1000-5/1)# ip access-group enable-deny-logging
```
ip access-group redirect-deny-to-interf

Redirects traffic with deny IPv4 ACL matches to an interface that you specify.

Syntax

```
ip access-group redirect-deny-to-interf slot / port

no ip access-group redirect-deny-to-interf slot / port
```

Command Default

No redirect is defined.

Parameters

`slot / port`

Specifies the interface to which denied traffic is redirected.

Modes

Interface subtype configuration modes

Usage Guidelines

Denied-traffic redirection is supported for inbound ACLs only.

VPLS, VLL, and VLL-local endpoints do not support the `ip access-group redirect-deny-to-interf` command.

Implementation of both deny-logging (`ip access-group enable-deny-logging`) and denied-traffic redirection on an interface can affect denied-traffic redirection. For rules that contain the log keyword, deny-logging prevents denied-traffic redirection.

To disable denied-traffic redirection, use the `no` form of this command (with `slot / port`).

Examples

The following example implements ACL denied-traffic redirection on an interface

```
device# configure terminal
device(config)# interface ethernet 5/2
device(config-if-e1000-5/2)# ip access-group redirect-deny-to-interf
```
**ip access-group ve-traffic**

Enables filtering of traffic switched within a virtual routing interface.

**Syntax**

```
ip access-group ve-traffic
no ip access-group ve-traffic
```

**Command Default**

ACLs do not filter traffic switched from one port to another within a virtual routing interface.

**Modes**

Virtual-routing interface mode

**Usage Guidelines**

This command does not affect ACLs applied to outbound traffic.

The **no** form of this command disables filtering of traffic switched within a virtual routing interface.

**Examples**

The first phase of the following example configures port-based VLAN 10, adds ports 1/1 through 2/12 to the VLAN, and then adds virtual routing interface 1 to the VLAN.

```
device# configure terminal
device(config)# vlan 10 name IP-subnet-vlan
device(config-vlan-10)# untag ethernet 1/1 to 1/20 ethernet 2/1 to 2/12
device(config-vlan-10)# router-interface ve 1
device(config-vlan-10)# exit
```

The second phase of the example configures a standard numbered IPv4 ACL, using the **access-list** command. (You can also use the **ip access list** and [ **sequence** ] { **permit** | **deny** } commands.)

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

The third phase of the example enables filtering of traffic switched within a virtual routing interface. It then applies the ACL, in an ingress direction, to a subset of the ports associated with virtual interface 1.

```
device(config)# interface ve 1
device(config-vif-1)# ip access-group ve-traffic
device(config-vif-1)# ip access-group 1 in ethernet 1/1 ethernet 1/3 ethernet 2/1 to 2/4
```
**ip access-list**

Creates a named or numbered IPv4 standard or extended access list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

**Syntax**

```
ip access-list { standard | extended } { acl-num | acl-name }
no ip access-list { standard | extended } { acl-num | acl-name }
```

**Command Default**

No IPv4 named or numbered ACLs are defined. However, you can also create numbered IPv4 ACLs, using the `access-list` command.

**Parameters**

- **standard**
  
  Creates a standard access list. Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified address.

- **extended**
  
  Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

- **acl-num**
  
  Specifies the ACL number for a standard or extended access list. The value can be from 1 through 99 for standard IPv4 ACLs and from 100 through 199 for extended IPv4 ACLs.

- **acl-name**
  
  Specifies a unique IPv4 ACL name. The name can be up to 255 characters, and must begin with an alphabetic character. If the name contains spaces, put it within quotation marks. Otherwise, no special characters are allowed, except for underscores and hyphens.

**Modes**

Global configuration mode

**Usage Guidelines**

An IPv4 ACL name must be unique among standard and extended ACL types.

After you create a named ACL, enter one or more `[sequence] { permit | deny }` commands to create filtering rules for that ACL.

An IPv4 ACL starts functioning only after it is applied to an interface using the `ip access-group` command.

The system supports the following IPv4 ACL resources:

- IPv4 numbered standard ACLs—99
- IPv4 numbered extended ACLs—100
• IPv4 named standard ACLs—100
• IPv4 named extended ACLs—500
• Maximum filter-rules per IPv4 or IPv6 ACL—4096. You can change the maximum up to 102400 by using the `system-max ip-filter-sys` command.

The **no** form of this command deletes the ACL. You can delete an IPv4 ACL only after you first remove it from all interfaces to which it is applied, using the **no ip access-group** command.

**Examples**

The following example creates a standard, named IPv4 ACL, defines rules in it, and applies it to an ethernet interface.

```
device(config)# ip access-list standard Net1
device(config-std-nacl-Net1)# deny host 10.157.22.26
device(config-std-nacl-Net1)# deny 10.157.29.12
device(config-std-nacl-Net1)# deny host IPHost1
device(config-std-nacl-Net1)# permit any
device(config-std-nacl-Net1)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group Net1 in
```

The following example creates an extended, named IPv4 ACL, defines rules in it, and applies it to an ethernet interface, in the ingress direction.

```
device(config)# ip access-list extended "block Telnet"
device(config-ext-nacl-block telnet)# deny tcp host 10.157.22.26 any eq telnet
device(config-ext-nacl-block telnet)# permit ip any any
device(config-ext-nacl-block telnet)# exit
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip access-group "block Telnet" in
```

The following example creates an extended, numbered IPv4 ACL and defines rules in it.

```
device# configure terminal
device(config)# ip access-list extended 101
device(config-ext-nacl-101)# seq 30 deny udp 19.1.2.0 0.0.0.255 eq 2023 20.1.2.0 0.0.0.255 eq 2025 dscp-mapping 23
device(config-ext-nacl-101)# permit 12 host 098.096.31.10 any
device(config-ext-nacl-101)# deny tcp host 098.092.12.10 131.21.12.0/24 syn
device(config-ext-nacl-101)# deny 120 host 18.192.112.110 13.2.2.0/24 log
device(config-ext-nacl-101)# permit ip any any mirror
```
ip access-list logging-age

Specifies, in minutes, how long the system waits before it sends a message in the Syslog.

Syntax

```
ip access-list logging-age minutes
no ip access-list logging-age minutes
```

Command Default

The default is five minutes.

Parameters

```
minutes
```

Specifies, in minutes, how long the system waits before it sends a message in the Syslog. Valid values range from 1 through 10. The default is five minutes.

Modes

Global configuration mode

Usage Guidelines

To reset the default value of five minutes, use the `no` form of this command.

Examples

The following example sets `logging-age` to two minutes.

```
device# configure terminal
device(config)# ip access-list logging-age 2
```
ip allow-src-multicast

   Allows packets with multicast addresses as source IP addresses.

Syntax

ip allow-src-multicast [decimal | all ]
no ip allow-src-multicast [decimal | all ]

Command Default

   Packets with multicast addresses as source IP addresses are not forwarded.

Parameters

decimal
   Specifies the slot number on which multicast addresses as source IP addresses should be allowed.

   all
   Specifies all slots on which multicast addresses as source IP addresses are allowed.

Modes

   Global configuration mode

Usage Guidelines

   The no form of this command disables multicast addresses as source IP addresses. You cannot configure the ip allow-src-multicast command along with the ip allow-src-multicast switched-traffic command on the same slot.

Examples

   The following example allows all multicast addresses as source IP addresses for all traffic and for all slots.

device(config)# ip allow-src-multicast all

   The following example shows allowing multicast IP addresses as source address for a particular slot.

device(config)# ip allow-src-multicast 2

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip allow-src-multicast switched-traffic

Disables packet drop for switched traffic only.

Syntax

ip allow-src-multicast switched-traffic [decimal | all]
nop ip allow-src-multicast switched-traffic [decimal | all]

Command Default

Packet drop for switched traffic is enabled.

Parameters

decimal
   Specifies the slot number on which the switched traffic should be allowed.

all
   Specifies all slots on which switched traffic is allowed.

Modes

Global configuration mode

Usage Guidelines

You cannot configure the ip allow-src-multicast switched-traffic command and ip allow-src-multicast command on the same slot. The no form of this command enables packet drop for switched traffic.

Examples

The following example allows multicast addresses as source IP addresses for switched traffic for a particular slot.

device(config)# ip allow-src-multicast switched-traffic 2

The following example allows multicast addresses as source IP addresses for switched traffic for all slots.

device(config)# ip allow-src-multicast switched-traffic all

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip arp-refresh-request-timer
Sets the ARP refresh request timer and enhances the ARP scaling number to 128k.

Syntax
ip arp-refresh-request-timer num

Command Default
The default value is 120 seconds.

Parameters
num
Timer setting in seconds. Possible values are 10 through 3600 seconds.

Modes
Global configuration mode.

Usage Guidelines
Use the default value as minimum the value in scaled configuration.
The ARP request timer must be greater than the ARP pending retry timer.

Examples
The following example sets the ARP refresh timer to 240 seconds.

device# configure terminal
device(config)# ip arp-refresh-request-timer 240

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
ip http client connection timeout connect

This command sets the maximum time for the client to wait for the connection to be established while initiating a connection to the HTTP(S) server.

Syntax

ip http client connection timeout connect seconds
no ip http client connection timeout connect

Parameters

seconds

Specifies the amount of time in seconds that the client will wait for the connection to be established with the HTTP(S) server. Can be an integer value from 1 to 15. The default value is 5.

Modes

Privileged EXEC mode

Usage Guidelines

no

Examples

The following example sets the time to the default value of 5 seconds.

device(config)# no ip http client connection timeout connect

The following example sets the time to 12 seconds.

device(config)# ip http client connection timeout connect 12

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**ip http client connection timeout idle**

This command sets the maximum time for the client to keep the connection to the http(s) server idle before closing the connection.

**Syntax**

```
ip http client connection timeout idle [ seconds ]
```

**Parameters**

- `seconds`

  Specifies the amount of time in seconds that the client will wait for the connection to be established with the http(s) server. Can be an integer value from 1 to 15. The default value is 5.

**Modes**

Privileged EXEC mode

**Usage Guidelines**

**Examples**

The following example sets the time to the default value of 5 seconds.

```
device(config)# ip http client connection timeout idle
```

The following example sets the time to 12 seconds.

```
device(config)# ip http client connection timeout idle 12
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**ip http client source-interface**

Configures the source-interface for the HTTP(S) client.

**Syntax**

```
ip http client source-interface { ethernet | loopback | ve } interface-number
```

**Parameters**

- `interface-number`
  
  Specifies the interface number for the source interface of the HTTP(S) client. When the `source-interface` is `ethernet`, the `interface-number` must be in the form `slot/port`. For loopback and logical interfaces, you must use an integer value for `interface-number`.

**Modes**

- Privileged EXEC mode

**Usage Guidelines**

**Examples**

The following example configures the source interface (slot 7, port 12) for the HTTP(S) client.

```
device(config)# ip http client source-interface ethernet 7/12
```

The following example configures the loopback interface for the HTTP(S) client.

```
device(config)# ip http client source-interface loopback 1
```

The following example configures the logical interface (2) for the HTTP(S) client.

```
device(config)# ip http client source-interface ve 2
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip multicast-routing fast-convergence

Enables fast convergence.

Syntax

ip multicast-routing fast-convergence
no ip multicast-routing fast-convergence

Command Default

Fast convergence is disabled.

Modes

Global configuration mode.

Usage Guidelines

When you enable fast convergence, each PIM join is sent immediately, which ensures faster convergence. However, enabling fast convergence also increases the number of PIM messages on the system. In systems with very high number of mcache entries, batching of PIM messages is recommended to reduce the number of periodic messages and for faster convergence.

The no form of the command disables fast convergence.

Examples

The following example configures fast convergence.

device# configure terminal
device(config)# ip multicast-routing fast-convergence

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip multicast-routing load-sharing

Enables or disables load distribution among IP ECMP paths.

Syntax

- **ip multicast-routing load-sharing [ rebalance ]**
- **no ip multicast-routing load-sharing [ rebalance ]**

Parameters

- **rebalance**
  Specifies that the ECMP load-sharing will be re-balanced for the interface on which the `rebalance` keyword is configured.

Modes

Interface configuration mode.

Examples

To configure Multicast ECMP, use this command in the configuration mode.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip multicast-routing load-sharing
```

To disable load distribution among ECMP IP paths use the `no` form of the command.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# no ip multicast-routing load-sharing
```

The following example configures re-balancing of the load distribution among ECMP IP paths.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip multicast-routing load-sharing rebalance
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip ospf bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv2 interface.

Syntax

ip ospf bfd disable
no ip ospf bfd

Command Default

BFD is disabled by default.

Parameters

disable

Disables BFD on the OSPFv2 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated if BFD is also enabled globally using the bfd all-interfaces command in OSPF router configuration mode. If BFD is disabled using the no bfd all-interfaces command in OSPF router configuration mode, BFD sessions on specific OSPFv2 interfaces are deregistered.

The no form of the command removes all BFD sessions from a specified interface.

Examples

The following example enables BFD on a specific OSPF Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf bfd

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

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf bfd disable
ip ospf cost

Configures cost for a specific interface.

Syntax

ip ospf cost value
no ip ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv2 cost on the interface. If the cost is not configured with this command, OSPFv2 calculates the value from the reference and interface bandwidths.

You can modify the cost to differentiate between 100 Mbps, 1 Gbps, and 10 Gbps. The default cost is calculated by dividing 100 million by the bandwidth. For 10 Mbps links, the cost is 10. The cost for 100 Mbps, 1 Gbps, and 10 Gbps links is 1, because the speed of 100 Mbps and 10 Gbps was not in use at the time the OSPF cost formula was devised.

The no form of the command disables the configured cost.

Examples

The following example sets the cost to 600 on a specific OSPFv2 Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf cost 600
ip ospf database-filter

Configures filters for different types of outgoing Link State Advertisements (LSAs).

Syntax

ip ospf database-filter all out
ip ospf database-filter all-external { allow-default out | allow-default-and-type-4 out | out }
ip ospf database-filter all-summary-external { allow-default out | allow-default-and-type-4 out | out }
no ip ospf database-filter all out
no ip ospf database-filter all-external
no ip ospf database-filter all-summary-external

Command Default

All filters are disabled.

Parameters

all out
Blocks all LSAs.

all-external
Blocks all external LSAs.

allow-default-and-type-4
Allows default-route LSAs and Type 4 LSAs, but block all other LSAs.

allow-default-out
Allows default-route LSAs, but block all other LSAs.

out
Filters outgoing LSAs.

all-summary-external
Blocks all summary (Type 3) and external (type 5) LSAs.

Modes

Interface subtype configuration mode

Usage Guidelines

By default, the device floods all outbound LSAs on all the OSPFv2 interfaces within an area. You can configure a filter to block outbound LSAs on an OSPF interface. This feature is particularly useful when you want to block LSAs from some, but not all, of the interfaces attached to the area. When enabled, this command blocks the specified outgoing LSAs on the interface. Some cases where you might want to enable filters are:

- To control the information being advertised to the network.
To use a passive router for debugging only.

Enter `no ip ospf database-filter` followed by the appropriate operands to disable this configuration.

NOTE

You cannot block LSAs on virtual links and LSA filtering is not supported on sham links.

**Examples**

To apply a filter to block flooding of all LSAs on a specific OSPF 40-gigabit Ethernet interface:

```
device(config)# interface fortygigabitethernet 101/0/10
device(config-if-fo-101/0/10)# ip ospf database-filter all-out
```

To apply a filter to block flooding of all LSAs on a specific OSPF virtual Ethernet (VE) interface:

```
device(config)# rbridge-id 178
device(config-rbridge-id-178)# interface ve 24
device(config-Ve-24)# ip ospf database-filter all-out
```
ip ospf dead-interval

Configures the neighbor dead interval, which is the number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ip ospf dead-interval interval
no ip ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 2147483647 seconds. The default is 40.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the ip ospf hello-interval command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The running-config command displays only explicitly configured values of the hello interval, which means that a value that was automatically changed as the result of a dead-interval change is not displayed.

The no form of the command restores the default value.

Examples

The following example sets the dead interval to 200 on a specific OSPFv2 Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf dead-interval 200
**ip ospf hello-interval**

Configures the hello interval, which is the length of time between the transmission of hello packets that this interface sends to
neighbor routers.

**Syntax**

```
ip ospf hello-interval interval
no ospf hello-interval
```

**Command Default**

The default value is 10 seconds.

**Parameters**

```
interval
```
Hello interval in seconds. Valid values range from 1 through 65535.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello
interval, unless the dead interval is also explicitly configured using the `ip ospf dead-interval` command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The `running-config` command displays only explicitly configured values of the dead interval, which means that a value that was
automatically changed as the result of a hello-interval change is not displayed.

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

**Examples**

The following example sets the hello interval to 50 on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf hello-interval 50
```
ip ospf md5-authentication

Configures MD5 password and authentication change hold time.

Syntax

ip ospf md5-authentication { key-activation-wait-time wait-time | key-id id MD5_key key password }

no ip ospf md5-authentication key-id

Command Default

No authentication.

Parameters

key-activation-wait-time wait-time
Sets the time that OSPFv2 waits before activating a new MD5 key. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends use the newly configured MD5 Key. OSPFv2 packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. Valid values range from 0 to 14400 seconds. The default value is 300 seconds.

key-id
Sets MD5 key and OSPFv2 password.

id MD5_key
The num is a number between 1 and 255 and identifies the MD5 key that is being used. This parameter is required to differentiate among multiple keys defined on a router. When MD5 is enabled, the key is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPFv2 packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication. By default, the MD5 authentication key is encrypted.

0 password
The key string is not encrypted and is in clear text.

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

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

ospf_password
OSPF processes password as a plain text password. OSPF internally encrypts this password as if encryption key 2 was specified and shows the encrypted password in the show running command output as follows:
key 2 $cilpVT0=

Modes

Interface subtype configuration mode
Usage Guidelines

Use this command to set or reset the MD5 password and/or authentication change hold time on the interface to which you are connected.

By default, the authentication key is encrypted. If you want the authentication key to be in clear text, insert a 0 between authentication-key and string. The software adds a prefix to the authentication key string in the configuration. For example, the following portion of the code has the encrypted code "2".

Enter `no ip ospf md5-authentication key-id` to disable this configuration.

Examples

The following example sets the time that OSPFv2 waits before activating a new MD5 key to 240.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ip ospf md5-authentication key-activation-wait-time 240
ip ospf mtu-ignore
Enables or disables maximum transmission unit (MTU) match checking.

Syntax
ip ospf mtu-ignore
no ip ospf mtu-ignore

Command Default
Enabled

Modes
Interface subtype configuration mode

Usage Guidelines
In default operation, the IP MTU on both sides of an OSPFv2 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The no form of the command disables MTU-match checking on a specific interface.

Examples
The following example disables MTU-match checking on a specific OSPFv2 Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# no ip ospf mtu-ignore

The following example enables MTU-match checking on a specific OSPFv2 Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf mtu-ignore
**ip ospf network**

Configures the network type for the interface. Point-to-point can support unnumbered links, which requires less processing by OSPF.

**Syntax**

```
ip ospf network { broadcast | non-broadcast | point-to-point }
```

no ip ospf network

**Command Default**

Network type is broadcast.

**Parameters**

- **broadcast**
  - Network type is broadcast.

- **non-broadcast**
  - Network type is non-broadcast. An interface can be configured to send OSPF traffic to its neighbor as unicast packets rather than multicast packets.

- **point-to-point**
  - Network type is point-to-point.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

On a non-broadcast interface, the devices at either end of the interface must configure non-broadcast interface type and the neighbor IP address. There is no restriction on the number of devices sharing a non-broadcast interface.

To configure an OSPF interface as a non-broadcast interface, the feature must be enabled on a physical interface or a VE, following the `ip ospf area` statement, and then specify the IP address of the neighbor in the OSPF configuration. The non-broadcast interface configuration must be done on the OSPF devices at either end of the link.

The `no` form of the command removes the network-type configuration.

**Examples**

The following example configures an OSPFv2 point-to-point link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf network point-to-point
```
The following example configures an OSPFv2 broadcast link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf network broadcast
```
ip ospf passive
    Sets a specific OSPFv2 interface to passive.

Syntax
    ip ospf passive
    no ip ospf passive

Command Default
    All OSPF interfaces are active.

Modes
    Interface subtype configuration mode

Usage Guidelines
    When you configure an OSPF interface to be passive, that interface does not send or receive OSPF route updates. Since a passive interface does not send or receive route information, the interface is in effect a stub network.

    You might want to set an interface to passive mode if:
    • You are planning to use the router mostly for debugging purposes.
    • The router is a stub and does not route traffic.

    The no form of the command sets an interface back to active.

Examples
    The following example sets a specific OSPFv2 Ethernet interface to passive.

    device# configure terminal
    device(config)# interface ethernet 1/1
    device(config-if-e1000/1/1)# ip ospf passive
ip ospf priority

Configures priority for designated router (DR) election.

Syntax

ip ospf priority value
no ip ospf priority

Command Default

The default value is 1.

Parameters

value

Priority value. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv2 router assigned the highest priority becomes the designated router, and the OSPFv2 router with the second-highest priority becomes the backup router.

If you set the priority to 0, the device does not participate in DR and BDR election.

The no form of the command restores the default value.

Examples

The following example sets a priority of 10 for the OSPFv2 router that is connected to an OSPFv2 Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf priority 10
ip ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

Syntax

```
ip ospf retransmit-interval interval
no ip ospf retransmit-interval
```

Command Default

The interval is 5 seconds.

Parameters

```
interval
```
Retransmit interval in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The no form of the command resets the retransmit interval to its default.

Examples

The following example sets the retransmit interval to 8 for all OSPFv2 devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf retransmit-interval 8
```
ip ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv2 to send link-state update packets on the interface to which you are connected.

Syntax

    ip ospf transmit-delay value
    no ip ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

    value

    Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

    Interface subtype configuration mode

Usage Guidelines

The no form of the command restores the default value.

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv2 Ethernet interface.

    device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ip ospf transmit-delay 25
ip rate-limit option-pkt-to-cpu policy-map

Applies rate-limit on IPv4 option packets.

Syntax

```
ip rate-limit option-pkt-to-cpu policy-map rate-limit policy
no ip rate-limit option-pkt-to-cpu policy-map rate-limit policy
```

Command Default

By default this command is disabled.

Parameters

```
policy-map rate-limit policy
```

Specifies the name of the policy-map.

Modes

Global configuration mode

Usage Guidelines

The no form of the command disables rate-limiting on IPv4 option packets.

Create CPU bound rate-limit policy map before applying rate-limiting for option packets.

**NOTE**

The following warning message is displayed if only some of the cards are supported and few are not supported.

```
Warning: rate-limit config for protocol "option-pkt-to-cpu" is not supported on module 1, 3
```

The following warning message is displayed if none of the cards are supported.

```
Warning: rate-limit config for protocol "option-pkt-to-cpu" is not supported on available modules. It is only supported on GEN-2 and later modules.
```

Examples

The following example explains how to apply rate-limit for IPv4 option packets.

```
device(config)#ip rate-limit option-pkt-to-cpu policy-map save-cpu-policy
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip rate-limit ttl-expired-to-cpu policy-map
Applies rate-limit option on IPv4 ttl packets, if the ttl count is less than or equal to one.

Syntax

ip rate-limit ttl-expired-to-cpu policy-map rate-limit policy
no ip rate-limit ttl-expired-to-cpu policy-map rate-limit policy

Command Default
By default this command is disabled.

Parameters

policy-map rate-limit policy
Specifies the name of the policy-map.

Modes
Global configuration mode

Usage Guidelines
The no form of the command disables rate-limit option on IPv4 ttl-expired-to-cpu packets.
Create a CPU bound rate-limit policy map before applying rate-limiting for ttl-expired-to-cpu packets.

NOTE
The following warning message is displayed if only some of the cards are supported and few are not supported.

Warning: rate-limit config for protocol "ttl-expired-to-cpu" is not supported on module 1, 3

The following warning message is displayed if none of the cards are supported.

Warning: rate-limit config for protocol "ttl-expired-to-cpu" is not supported on available modules. It is only supported on GEN-2 and later modules.

Examples
The following example explains how to apply rate-limit option on IPv4 ttl-expired-to-cpu packets.

device(config)# ip rate-limit ttl-expired-to-cpu policy-map save-cpu-policy

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip receive access-list

Configures an IPv4 access-control list as an IPv4 receive access-control list (rACL).

Configures an IPv4 access-list as IPv4 rACL. The IPv4 traffic matching the "permit" clause specified in the IPv4 ACL is permitted and IPv4 traffic matching the "deny" clause in the IPv4 ACL is dropped into the hardware.

Syntax

ip receive access-list { acl-num | acl-name } sequence seq-num [ policy-map policy-map-name [ strict-acl ] ]
no ip receive access-list { acl-num | acl-name } sequence seq-num [ policy-map policy-map-name [ strict-acl ] ]

Parameters

 acl-num | acl-name Specifies, in number or name format, the access-control list to apply to all interfaces within the default VRF, for all CPU-bound traffic.
 sequence seq-num Defines the sequence number of the access-control list being applied as a rACL. IPv4 rACL commands are applied in the order of the lowest to the highest sequence numbers. The range of values is from 1 through 200.
 policy-map policy-map-name Specifies the name of a policy map. When the policy-map option is specified, traffic matching the "permit" clause of the specified IPv4 ACL is rate-limited as defined in the policy map and IPv4 traffic matching the "deny" clause in the IPv4 ACL is permitted without rate limiting.
 strict-acl Specifies that traffic matching the "permit" clause of the specified IPv4 ACL is rate-limited as defined in the policy map and IPv4 traffic matching the "deny" clause in the IPv4 ACL is dropped into the hardware.

Modes

Global configuration mode.

Usage Guidelines

The no form of the basic command removes the rACL.

The no form of the command with both policy-map and strict-acl options specified, removes the strict-acl option: the rACL with policy-map remains and traffic matching "deny" clauses starts passing to the CPU.

Examples

The following example configures the IPv4 ACL "101" as a rACL with the sequence number "15".

device(config)# ip receive access-list 101 sequence 15

The following example configures the IPv4 ACL "acl_stand1" as an rACL with the sequence number "10".

device(config)# ip receive access-list acl_stand1 sequence 10

The following example removes the strict-acl option so that traffic matching "deny" clauses starts passing to the CPU: the rACL "acl_stand1" with the policy map "m1" remains.

device(config)# no ip receive access-list acl_stand1 sequence 10 policy-map m1 strict-acl
### History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was modified to support named rACLs.</td>
</tr>
</tbody>
</table>
ip route bfd

Enables Bidirectional Forwarding Detection (BFD) monitoring for an IP static route.

Syntax

```
ip route A.B.C.D/L A.B.C.D bfd [ metric | distance number | name name | tag number
```

Command Default

BFD monitoring for an IP static route is not enabled.

Parameters

- **A.B.C.D/L**
  - Specifies the destination IPv4 address and mask.
- **A.B.C.D**
  - Specifies the IPv4 address of the next hop.
- **metric**
  - Specifies the cost metric of the route. Valid values range from 1 through 16. The default is 1.
- **distance number**
  - Specifies the administrative distance of the route. Valid values range from 1 through 255. The default is 1.
- **name name**
  - Specifies the name of the route in ASCII characters.
- **tag number**
  - Specifies the tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes BFD monitoring from the static route.

Examples

The following example enables BFD route monitoring on an IP static route and sets the cost metric of the route to 8.

```
device# configure terminal
device(config)# ip route 10.1.0.0/24 10.2.0.5 bfd 8
```

The following example enables BFD route monitoring on an IP static route and sets the administrative distance of the route to 60.

```
device# configure terminal
device(config)# ip route 10.0.0.0/24 10.0.0.5 bfd distance 60
```
The following example enables BFD route monitoring on an IP static route and sets the name of the route to "route1".

```
device# configure terminal
device(config)# ip route 10.0.2.0/24 10.0.3.5 bfd name route1
```

The following example enables BFD route monitoring on an IP static route and sets the tag value of the route to 10.

```
device# configure terminal
device(config)# ip route 10.0.2.0/24 10.0.3.5 bfd tag 10
```
ip route static-bfd

Configures Bidirectional Forwarding Detection (BFD) session parameters for IP static routes.

Syntax

```
ip route [ vrf vrf-name ] static-bfd dest-ip-address source-ip-address [ interval transmit-time min-rx receive-time multiplier number ]
oip route [ vrf vrf-name ] static-bfd dest-ip-address source-ip-address
```

Command Default

BFD is not configured for an IP static route.

Parameters

- **vrf vrf-name**
  - Specifies the name of a VRF instance.

- **dest-ip-address**
  - Specifies the destination IP address.

- **source-ip-address**
  - Specifies the source IP address.

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

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

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

Modes

- Global configuration mode

Usage Guidelines

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

For single-hop static BFD sessions, timeout values are optional because all required information is available from the outgoing interface. For multihop BFD sessions, if the configured interval and min-rx parameters conflict with those of an existing BGP session, the lower values are used.
If you configure a neighbor IP address and a source IP address that already exist in BFD, BFD overwrites the existing interval values and multiplier for the IP addresses with the new values on behalf of the static module.

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

The no form of the command disables BFD monitoring by removing the BFD static neighbor and eliminating the BFD session, while keeping the static route in the route table manager (RTM), and retaining the existing IP traffic route. You only need to specify the destination and source IP address when removing a BFD neighbor.

Examples

The following example configures a BFD session on an IP static route.

device# configure terminal
device(config)# ip route static-bfd 10.0.2.1 10.1.1.1 interval 500 min-rx 500 multiplier 5
ip ssh encryption disable-aes-cbc

Disables the Advanced Encryption Standard - Cipher-Block Chaining (AES-CBC) encryption mode for the Secure Shell (SSH) protocol.

Syntax

ip ssh encryption disable-aes-cbc

no ip ssh encryption disable-aes-cbc

Command Default

If JITC is enabled, only AES-CTR encryption mode is supported and AES-CBC mode is disabled by default. In the standard mode, the AES-CBC encryption mode is enabled.

Modes

Global configuration mode.

Usage Guidelines

The no form of the command enables the AES-CBC encryption mode.

Examples

The following example disables the AES-CBC encryption mode.

device# configure terminal
device(config)# ip ssh encryption disable-aes-cbc

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip tcp adjust-mss
Configures the TCP MSS value of the IP TCP synchronization packets passing through a router.

Syntax
ip tcp [ adjust-mss max-segment-size ]
no ip tcp [ adjust-mss max-segment-size ]

Command Default
Configuring the TCP MSS value of the IP TCP synchronization packets is not enabled by default.

Parameters
- **adjust-mss**: Specifies the TCP MSS value configuration parameter.
- **max-segment-size**: Specifies the maximum segment size in bytes. The range is from 512 - 9158 bytes. Since the range is based on configuration of the IP MTU or GRE Tunnel MTU value, the CLI does not display the configurable range.

Modes
Interface level, and virtual interface (VE) level.

Usage Guidelines

For a GRE tunnel, the `ip tcp adjust-mss` command is supported only on Gen-2 Switch Fabric Modules and later.

Use the `ip tcp adjust-mss` command to modify the TCP MSS value of the IP TCP synchronization packets passing through a router. Please note that the TCP MSS is applicable only for inbound traffic. When you configure the IP MTU value on the same Ethernet interface as the configured TCP MSS value, the software internally modifies the TCP MSS value according to the current IP MTU value so dropped or fragmented packets are avoided. The TCP MSS value is modified based on the IP MTU or GRE tunnel MTU configuration. If the configured TCP MSS value is less than the current IP MTU value or GRE tunnel MTU value, then the software will not modify the TCP MSS value. Refer to the examples below for modifying the TCP MSS value based on the IP MTU configuration or the GRE tunnel MTU configuration.

**Modifying the TCP MSS value based on the IP MTU configuration**

For example, on ethernet interface 1/1 the TCP MSS is configured to 1400 bytes. If you configure the IP MTU value to 1000 bytes on ethernet interface 1/1, the software internally modifies the TCP MSS value to 960 bytes. The TCP MSS value modification is required by software because the configured TCP MSS value (1400 bytes) is greater than the user configuration of the IP MTU value. The modified value is calculated by subtracting the user configuration from the current IP MTU value - 1000 bytes minus 40 bytes equals 960 bytes.

**Modifying the TCP MSS value based on the GRE tunnel MTU configuration**

For example, on ethernet interface 1/1 the TCP MSS value is configured to 1400 bytes. The ethernet interface 1/1 is a tunnel source for the GRE tunnel 100. If you configure the GRE tunnel MTU value to 700 bytes on ethernet interface 1/1, the software internally modifies the TCP MSS value to 660 bytes. The TCP MSS value modification is required by software because the configured TCP MSS value (1400 bytes) is greater than the user configuration of the GRE tunnel MTU value. The modified...
value is calculated by subtracting the user configuration from the current GRE tunnel MTU value - 700 bytes minus 40 bytes equals 960 bytes.

After configuring the \texttt{ip tcp adjust-mss max-segment-size} command, and the \texttt{ip tcp redirect-gre-tcp-syn} command, the hardware redirects the TCP SYN packets received on interface port 1/1 to the LP software. The LP software adjusts the TCP MSS value in the incoming packet.

The GRE tunnel MTU configuration takes a higher priority over the IP MTU configuration. If the GRE tunnel MTU is not configured, then the IP MTU configuration is used to modify the TCP MSS value. The \texttt{ip tcp adjust-mss max-segment-size} command can only enabled on the GRE ingress interface. The TCP MSS value is modified only in the source port of the ingress GRE tunnel. The TCP MSS value cannot be modified when the tunnel source port is configured as an IP address port. The \texttt{ip tcp adjust-mss max-segment-size} command is supported only on an IPv4 interface.

Use the \texttt{no} form of the command to disable the TCP MSS value configuration parameter. Backward compatibility is not supported.

\textbf{NOTE}

Configuring the TCP MSS value is supported only on the Brocade Netiron XMR Series and the Brocade NetIron MLX Series platforms.

\section*{Examples}

The following example configures the TCP MSS value to 1000 bytes.

```
device(config)# interface ethernet 2/1
device(config-if-e10000-2/1)# ip tcp adjust
adjust-mss Configure the TCP MSS
device(config-if-e10000-2/1)# ip tcp adjust-mss 10
Error - 10 not between 536 and 1460
device(config-if-e10000-2/1)# ip tcp adjust-mss 1000
device(config-if-e10000-2/1)#
```

Use the \texttt{show run interface} command to display the TCP MSS configuration on interface ethernet 2/1.

```
device(config-if-e10000-2/1)# show run interface
interface management 1
ip address x.x.x.x/24
enable

! interface ethernet 2/1
ip tcp adjust-mss 1000
!
interface ethernet 2/3
ip address x.x.x.x/24
!
interface ethernet 2/4
enable
```

\section*{History}

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip tcp redirect-gre-tcp-syn

Configures the GRE-based TCP synchronization packets to the CPU when the TCP MSS value is adjusted.

Syntax

    ip tcp [ redirect-gre-tcp-syn ]
    no ip tcp [ redirect-gre-tcp-syn ]

Command Default

Configuring the GRE based TCP synchronization packets to the CPU is not enabled by default.

Parameters

    redirect-gre-tcp-syn
        Specifies the GRE-based TCP synchronization packets parameter.

Modes

Global configuration mode.

Usage Guidelines

Use the `ip tcp redirect-gre-tcp-sync` command to optionally redirect the GRE-based TCP synchronization packets to the CPU when the TCP MSS value is adjusted. To redirect the GRE based TCP synchronization packets to the CPU, use the `ip tcp adjust-mss max-segment-size` command, and the `ip tcp redirect-gre-tcp-sync` command. To redirect only the IP TCP synchronization packets to the CPU, use `ip tcp adjust-mss max-segment-size` command.

After configuring the `ip tcp adjust-mss` command with the `max-segment-size` option, and the `ip tcp redirect-gre-tcp-sync` command, the hardware redirects the TCP SYN packets received on interface port 1/1 to the LP software. The LP software adjusts the TCP MSS value in the incoming packet. For more information on the `ip tcp adjust-mss max-segment-size` command, refer to the `ip tcp adjust-mss` command.

Use the `no` form of the command to disable the configuration of the GRE based TCP synchronization packets to the CPU. Backward compatibility is not supported. If the `ip tcp redirect-gre-tcp-sync` command is not configured, the incoming packet still receives the CPU for MAC learning.

You can optionally trap the TCP SYN packet in a GRE transit router by creating a dummy GRE tunnel in the transit router. For example, port 1/1 is the ingress port and port 1/2 is the egress port for the GRE based TCP SYN packets incoming and outgoing transmission. To trap the TCP SYN packets to the LP CPU on port 1/1, you need to create a dummy GRE tunnel in the configured tunnel source port, either port 1/1 or port 1/2.

**NOTE**

Configuring the GRE based TCP synchronization packets is supported only on the Brocade NetIron XMR Series and the Brocade NetIron MLX Series platforms.
Examples

The following example configures the GRE based TCP synchronization packets to the CPU on the global interface level.

```bash
device(config)# ip tcp redirect-gre-tcp-syn ?
redirect-gre-tcp-syn   Control the GRE based TCP Synchronization packets
device(config)# ip tcp redirect-gre-tcp-syn
device(config)#
```

Use the `show running-configuration` command to display the GRE based TCP synchronization packets configuration.

```bash
device# show running-config
!
hostname dut3
acl-duplication-check
ip multicast-routing
ip tcp redirect-gre-tcp-syn
!
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ip vrrp auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol (VRRP) interface.

Syntax

ip vrrp auth-type { no-auth | simple-text-auth auth-text }
no ip vrrp auth-type { no-auth | simple-text-auth auth-text }

Command Default

No authentication type is configured on a VRRP interface.

Parameters

no-auth

Configures no authentication on the VRRP interface.

simple-text-auth auth-text

Configures a simple text string as a password used for authenticating packets on the interface. The maximum length of the text string is 64 characters.

Modes

Interface configuration mode

Usage Guidelines

If the no-auth option is configured, ensure that all interfaces on all devices that support the virtual router ID do not use authentication.

If the simple-text-auth option is configured, ensure that all interfaces on all devices that support the virtual router ID are configured to use simple password authentication with the same password.

The no form of this command removes the VRRP authentication from the interface.

NOTE

Authentication is not supported by VRRP-Ev3.

Examples

The following example configures no authentication on Ethernet interface 1/6.

device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp auth-type no-auth

The following example configures simple password authentication on Ethernet interface 1/6.

device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp auth-type simple-text-auth yourpwd
ip vrrp vrid

Configures an IPv4 Virtual Router Redundancy Protocol (VRRP) virtual router identifier (VRID).

Syntax

ip vrrp vrid vrid
no ip vrrp vrid vrid

Command Default

A VRRP VRID does not exist.

Parameters

vrid

Configures a number for the IPv4 VRRP VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that VRRP is enabled globally; otherwise, an error stating "Invalid input..." is displayed as you try to create a VRRP instance.

The no form of this command removes the IPv4 VRRP VRID from the configuration.

Examples

The following example configures VRRP virtual router ID 1.

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

Configures the type of authentication used on a Virtual Router Redundancy Protocol Extended (VRRP-E) interface.

Syntax

ip vrrp-extended auth-type { no-auth | simple-text-auth auth-text | md5-auth auth-text }
no ip vrrp-extended auth-type { no-auth | simple-text-auth auth-text | md5-auth auth-text }

Command Default

No authentication is configured for a VRRP-E interface.

Parameters

no-auth
Configures no authentication on the VRRP-E interface.

simple-text-auth auth-text
Configures a simple text string as a password used for authenticating packets on the interface. The maximum length of the text string is 64 characters.

md5-auth auth-text
Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

Modes

Interface configuration mode

Usage Guidelines

If the simple-text-auth option is configured, ensure that all interfaces on all devices that support the virtual router ID are configured to use simple password authentication with the same password.

If the md5-auth option is configured, syslog and SNMP traps are generated if a packet is being dropped due to MD5 authentication failure. Using MD5 authentication implies that the software does not need to run checksum verification on the receiving device and can rely on the authentication code (message digest 5 algorithm) to verify the integrity of the VRRP-E message header.

Use the show run command with appropriate parameters to display the encrypted password; use the enable password-display command to display the unencrypted password.

If the no-auth option is configured, ensure that all interfaces on all devices that support the virtual router ID do not use authentication.

The no form of this command removes the VRRP-E authentication from the interface.

NOTE
Authentication is not supported by VRRP-Ev3.
Examples

The following example configures no authentication on Ethernet interface 1/6.

device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp-extended auth-type no-auth

The following example configures simple password authentication on Ethernet interface 1/6.

device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp-extended auth-type simple-text-auth yourpwd

The following example configures MD5 authentication on Ethernet interface 1/6. When MD5 authentication is configured, a syslog message is displayed.

device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip vrrp-extended auth-type md5-auth lyk28d3j

Aug 10 18:17:39 VRRP: Configuration VRRP_CONFIG_MD5_AUTHENTICATION request received
Aug 10 18:17:39 VRRP: Port 1/6, VRID 2 - send advertisement
Ver:3 Type:1 Vrid:2 Pri:240 #IP:1 AuthType:2 Adv:1 Chksum:0x0000
HMAC-MD5 CODE:[000000000000000000400010]
IpAddr: 10.53.5.1
ip vrrp-extended vrid


Syntax

ip vrrp-extended vrid vrid
no ip vrrp-extended vrid vrid

Command Default

A VRRP-E VRID does not exist.

Parameters

vrid

Configures a number for the IPv4 VRRP-E VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that VRRP-E is enabled globally; otherwise an error stating "Invalid input..." is displayed as you try to create a VRRP-E instance.

The no form of this command removes the IPv4 VRRP-E VRID from the configuration.

Examples

The following example configures VRRP-E VRID 1.

device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.10.1/24
device(config-if-e1000-1/6)# ip vrrp-extended vrid 1
device(config-if-e1000-1/6-vrid-1)# backup priority 50 track-priority 10
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.10.254
device(config-if-e1000-1/6-vrid-1)# activate
ip-address
Configures a virtual IP address for a Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) instance.

Syntax

```
ip-address ip-address
no ip-address ip-address
```

Command Default
A virtual IP address is not configured for a VRRP or VRRP-E instance.

Parameters

`ip-address`
Configures the IP address, in dotted-decimal format.

Modes
VRID interface configuration mode

Usage Guidelines
For VRRP instances, the IP address used for the virtual router must be configured on the device assigned to be the initial VRRP owner device. The same IP address cannot be used on any other VRRP device.

For VRRP-E instances, the IP address used for the virtual router must not be configured on any other device.

The no form of this command removes the virtual router IP address.

Examples

The following example configures a virtual IP address for VRID 1 when VRRP is implemented. In this example, the device is configured as the VRRP owner device.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
VRRP router 1 for this interface is activating
```
The following example configures a virtual IP address for VRID 2 when VRRP-E is implemented. In this example, the device is configured as a VRRP backup device and the highest priority device will become the master VRRP device.

device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 110
device(config-if-e1000-1/5-vrid-2)# version 2
device(config-if-e1000-1/5-vrid-2)# ip-address 10.53.5.254
device(config-if-e1000-1/5-vrid-2)# activate
VRRP router 2 for this interface is activating
ipsec profile

Creates an IP security (IPsec) profile and enters IPsec profile configuration mode.

Syntax

```
ipsec profile name
no ipsec profile name
```

Command Default

No IPsec profile is configured.

Parameters

`name`

Specifies the name of an IPsec profile.

Modes

Global configuration mode

Usage Guidelines

An IPsec profile defines parameters for encrypting communications between IPsec peer devices.

The `no` form of the command removes the specified IPsec profile configuration.

Examples

The following example shows how to create an IPsec profile named `ipsec_profile` and enters IPsec profile configuration mode for the profile.

```
device(config)# ipsec profile ipsec_profile
device(config-ipsec-profile-ipsec_profile)#
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipsec proposal

Creates an IP security (IPsec) proposal and enters IPsec proposal configuration mode.

Syntax

```plaintext
ipsec proposal name
```

Parameters

- **name**
  - Specifies the name of an IPsec proposal.

Modes

- Global configuration mode

Usage Guidelines

An IPsec proposal defines an encryption algorithm, encapsulation mode, and transform set used to negotiate with a data path peer. An IPsec proposal is activated by attaching it to an IPsec profile.

Examples

The following example creates an IPSec proposal named ipsec_proposal and enters IPsec proposal configuration mode for the proposal.

```plaintext
device(config)# ipsec proposal ipsec_proposal
device(config-ipsec-proposal-ipsec_proposal)#
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipsec self-sa-learning-enable

Enables learning of the Brocade device’s self MAC addresses whenever IP packets are received over the IPsec tunnel. This command supports IPv4 IPsec and IPv6 IPsec.

Syntax

ipsec self-sa-learning-enable
no ipsec self-sa-learning-enable

Command Default

By default, this option is not enabled.

Modes

Global configuration mode

Usage Guidelines

Enable this option in situations in which encrypted or decrypted IP packets are looped back to the system (device) for an additional level of encryption and decryption. IP packets that are looped back to the device are not sent to the CPU for learning of the device’s self MAC addresses.

When you enable this option, learning of the Brocade device’s self MAC addresses is enabled for all configured IPsec IPv4 and IPv6 tunnels on the device.

The no version of this command disables the learning of the Brocade device’s self MAC addresses.

Make sure you disable this option if you no longer need learning of the Brocade device’s self MAC addresses enabled.

Examples

The following example enables the learning of the Brocade device’s self MAC addresses for all configured IPsec IPv4 and IPv6 tunnels on the device.

Need complete example that contains all of the commands to: 1. Enter the mode required to configure the ipsec node. 2. Configure the ipsec node. 3. Enter the correct mode to enable the ipsec self-sa-learning-enable option. 4. Enable the ipsec self-sa-learning-enable option. (I have this command.)

device(config)# ipsec self-sa-learning-enable

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipv6 access-list

Creates an IPv6 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify. IPv6 ACLs filter traffic only after you apply them to interfaces.

Syntax

```
ipv6 access-list acl-name

no ipv6 access-list acl-name
```

Command Default

There are no default IPv6 ACLs.

Parameters

`acl-name`

Specifies a unique IPv6 ACL name. The name can be up to 199 consecutive characters (no spaces), and must begin with an alphabetic character. No special characters are allowed, except for underscores and hyphens. The string “test” is a reserved string.

Modes

Global configuration mode

Usage Guidelines

For IPv6 ACLs, only named ACLs are supported.

For IPv6 ACLs, only extended ACLs are supported. Extended ACLs contains rules that permit or deny traffic according to source and destination addresses, port protocol, and other IPv6 frame content.

After you create an IPv6 ACL, use the `sequence` `{ permit | deny }` command to create filtering rules for that ACL.

An IPv6 ACL starts functioning only after it is applied to an interface, using the `ipv6 traffic-filter` command.

The system supports the following IPv6 ACL resources:

- IPv6 named ACLs—1000
- Maximum filter-rules per IPv4 or IPv6 ACL—4096. You can change the maximum up to 102400 by using the `system-max ip-filter-sys` command.

To delete an IPv6 ACL, use the `no` form of this command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the `no ipv6 traffic-filter` command.
Examples

The following example creates an IPv6 ACL, defines within it a rule that blocks all Telnet traffic received from IPv6 host 2000:2382:e0bb::2, and applies the ACL to port 1/1.

device# configure terminal
device(config)# ipv6 access-list fdry
device(config-ipv6-access-list-fdry)# deny tcp host 2000:2382:e0bb::2 any eq telnet
device(config-ipv6-access-list-fdry)# permit ipv6 any any
device(config-ipv6-access-list-fdry)# exit
device(config)# interface ethernet 1/1
device(config-if-1/1)# ipv6 traffic-filter fdry in
device(config-if-1/1)# exit
device(config)# write memory

The first phase of the following example creates an IPv6 ACL, and defines the following rules within:

- Permit ICMP traffic from hosts in the 2000:2383:e0bb::/64 network to hosts in the 2001:3782::/64 network.
- Deny all IPv6 traffic from host 2000:2383:e0ac::2 to host 2000:2383:e0aa:0::24.
- Deny all UDP traffic.
- Permit all packets that are not explicitly denied by the other entries. (Without this entry, the ACL denies all incoming or outgoing IPv6 traffic on the ports to which the ACL is assigned.) Priority-mapping filters IPv6 traffic on the basis of the .1p priority.

device# configure terminal
device(config)# ipv6 access-list netw
device(config-ipv6-access-list-netw)# permit icmp 2000:2383:e0bb::/64 2001:3782::/64
device(config-ipv6-access-list-netw)# deny ipv6 host 2000:2383:e0ac::2 host 2000:2383:e0aa:0:24
device(config-ipv6-access-list-netw)# deny udp any any
device(config-ipv6-access-list-netw)# permit ipv6 any any priority-mapping 4
device(config-ipv6-access-list-netw)# exit

The second phase of the example applies the ACL to both incoming and outgoing traffic on port 1/2 and to incoming traffic on port 4/3.

device(config)# interface ethernet 1/2
device(config-if-1/2)# ipv6 traffic-filter netw in
device(config-if-1/2)# ipv6 traffic-filter netw out
device(config-if-1/2)# exit
device(config)# interface ethernet 4/3
device(config-if-4/3)# ipv6 traffic-filter netw in
device(config-if-4/3)# exit
device(config)# write memory
ipv6-address

Configures a virtual IPv6 address for a Virtual Router Redundancy Protocol version 3 (VRRPv3) or VRRP Extended version 3 (VRRP-Ev3) instance.

Syntax

ipv6-address { ipv6-address | auto-gen-link-local }

no ipv6-address { ipv6-address | auto-gen-link-local }

Command Default

A virtual IPv6 address is not configured for a VRRPv3 or VRRP-Ev3 instance.

Parameters

ipv6-address

Configures an IPv6 address.

auto-gen-link-local

Automatically generates a virtual IPv6 link-local address for the VRRPv3 instance. Not supported in VRRP-Ev3.

Modes

Virtual routing ID interface configuration mode

Usage Guidelines

For VRRP instances, the IPv6 address used for the virtual router must be configured on the device assigned to be the initial VRRP owner device. The same physical IPv6 address cannot be used on any other VRRP device.

If the auto-gen-link-local keyword is entered, a virtual IPv6 link-local address is generated automatically for the specific VRRPv3 instance. The virtual link-local address is carried in VRRPv3 advertisements. A manually configured link-local address takes precedence over the automatically generated address.

NOTE

Automatically generated virtual link-local addresses are not supported for VRRP-Ev3 instances.

The no form of the command removes the virtual router IPv6 address. If the auto-gen-link-local keyword was active, the automatically generated virtual IPv6 link-local address is removed for the VRRPv3 instance, and subsequent VRRPv3 advertisements will not carry this link-local address.
Examples

The following example configures a virtual IPv6 address for VRID 1 when IPv6 VRRPv3 is implemented. In this example, the device is configured as the VRRPv3 owner device.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ipv6 address fd2b::1/64
device(config-if-e1000-1/6)# ipv6 vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ipv6-address fe80::768e:f8ff:fe2a:0099
device(config-if-e1000-1/6-vrid-1)# ipv6-address fd2b::1
device(config-if-e1000-1/6-vrid-1)# activate
```

The following example automatically configures a virtual IPv6 link-local address for VRID 1 when an IPv6 VRRPv3 instance is activated. In this example, the device is configured as the VRRPv3 owner device.

```
NOTE
Automatically generated virtual IPv6 link-local addresses are not supported for VRRP-Ev3 instances.
```

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(conf-if-e1000-1/6)# ipv6 address fd2b::1/64
device(conf-if-e1000-1/6)# ipv6 vrrp vrid 1
device(conf-if-e1000-1/6-vrid-1)# owner
device(conf-if-e1000-1/6-vrid-1)# ipv6-address-auto-gen-link-local
device(conf-if-e1000-1/6-vrid-1)# ipv6-address fd2b::1
device(conf-if-e1000-1/6-vrid-1)# activate
```

The following example configures a virtual IPv6 address for VRID 2 when VRRP-Ev3 is implemented. In this example, the device is configured as a VRRP-Ev3 backup device and the highest priority device will become the master VRRP-Ev3 device.

```
device# configure terminal
device(config)# ipv6 router vrrp-extended
device(config-ipv6-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 address fd4b::1/64
device(config-if-e1000-1/5)# ipv6 vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 110
device(config-if-e1000-1/5-vrid-2)# ipv6-address fe80::768e:f8ff:fe3a:0099
device(config-if-e1000-1/5-vrid-2)# ipv6-address fd4b::99
device(config-if-e1000-1/5-vrid-2)# activate
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to add the <code>auto-gen-link-local</code> keyword that auto-generates an IPv6 virtual link-local address.</td>
</tr>
</tbody>
</table>
**ipv6 dhcp-relay include-options**
Includes the parameters on the IPv6 DHCP relay agent messages.

**Syntax**

```
ipv6 dhcp-relay include-options [ interface-id ] [ remote-id ] [ client-mac-address ]
no ipv6 dhcp-relay include-options [ interface-id ] [ remote-id ] [ client-mac-address ]
```

**Command Default**
The parameters are not included on the IPv6 DHCP relay agent messages.

**Parameters**

- **interface-id**
  Includes the interface-ID parameter (option 18) in the IPv6 DHCP relay agent messages.

- **remote-id**
  Includes the remote-ID (option 37) parameter in the IPv6 DHCP relay agent messages.

- **client-mac-address**
  Includes the client link layer address (option 79) in the relay-forward messages.

**Modes**
Interface configuration mode

**Usage Guidelines**
The interface-ID parameter on the DHCPv6 relay forward message is used to identify the interface on which the client message is received. By default, this parameter is included only when the client message is received with the link-local source address.

You can enter either one or all of the include options as identifiers to specify in the relay-forward message.

The **no** form of the command disables the relay agent include options parameters.

**Examples**
The following example includes the **client-mac-address** parameter on the DHCPv6 relay agent messages.

```
device(config)# interface ethernet 1/3
device(config-if-eth-1/3)# ipv6 dhcp-relay include-options client-mac-address
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9</td>
<td>This command was modified.</td>
</tr>
</tbody>
</table>
**ipv6 mroute**

Configures a multicast IPv6 static route for an interface.

**Syntax**

```plaintext
ipv6 mroute dest-ipv6-prefix/prefix-length [ ve ve-id | ipv6_tnl tunnel-id | 6to4_tnl tunnel_id ] [ next-hop-ipv6-address ]
[ metric ] [ distance number ] [ tag tag-number ] [ name string ]

ipv6 mroute dest-ipv6-prefix/prefix-length [ ethernet slot/port [ next-hop-ipv6-address ] ] [ metric ] [ distance number ] [ tag tag-number ]

ipv6 mroute ipv6-prefix/prefix-length next-hop-vrf vrf_name next-hop-ipv6-address [ metric ] [ distance number ] [ tag tag-number ]

ipv6 mroute dest-ipv6-prefix/prefix-length null0 [ metric ] [ distance number ] [ tag tag-number ]

no ipv6 mroute dest-ipv6-prefix/prefix-length [ ve ve-id | ipv6_tnl tunnel-id | 6to4_tnl tunnel_id ] [ next-hop-ipv6-address ]
[ metric ] [ distance number ] [ tag tag-number ] [ name string ]

no ipv6 mroute dest-ipv6-prefix/prefix-length [ ethernet slot/port [ next-hop-ipv6-address ] ] [ metric ] [ distance number ] [ tag tag-number ] [ name string ]

no ipv6 mroute ipv6-prefix/prefix-length next-hop-vrf vrf_name next-hop-ipv6-address [ metric ] [ distance number ] [ tag tag-number ]

no ipv6 mroute dest-ipv6-prefix/prefix-length null0 [ metric ] [ distance number ] [ tag tag-number ]
```

**Command Default**

An IPv6 static route is not configured.

**Parameters**

- `dest-ipv6-prefix`
  Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

- `prefix-length`
  A decimal value specifying the length of the IPv6 prefix.

- `next-hop-ipv6-address`
  IPv6 address of the next-hop gateway.

- `next-hop-vrf vrf_name next-hop-ipv6-address`
  Specifies a VRF instance and a next-hop IPv6 address.

- `null0`
  Causes packets to the selected destination to be dropped by shunting them to the "null0" interface. (This is the only available option.)

- `ethernet slot/port`
  Specifies the Ethernet slot or port.

- `ve ve-id`
  Specifies the virtual Ethernet (VE) interface VE ID.
6to4_tnl tunnel-id
   Specifies IPv6 to IPv4 tunnel number to be used as next hop.

ipv6_tnl tunnel-id
   Specifies IPv6 tunnel to be used as next hop.

name string
   Optional name (ASCII string) assigned to the route.

metric
   Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance number
   Specifies an administrative distance. The range is from 1 through 255. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route.

tag
   Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv6 static route redistribution).

tag-number
   A number from 0 through 4294967295. The default is 0.

Modes
   Global configuration mode
   VRF configuration mode

Usage Guidelines
   The no form of the command removes the multicast static route. If the route is named, the no form of the command must be used twice, the first time to remove the name and the second time to remove the route.

   The ethernet slot/port designation for the destination does not apply to PIM SM.

Examples
   The following example configures an IPv6 static route by specifying the destination prefix and the outgoing interface.

   device# configure terminal
device(config)#vrf green
device(config-vrf-green)#address-family ipv6
device(config-vrf-green-ipv6)#ipv6 mroute 2002::/64 eth 1/1
The static route can also be configured with outgoing interface as `ve`, such as `ve 10` as shown in the following example.

device# configure terminal
device(config)#vrf green
device(config-vrf-green)#address-family ipv6
device(config-vrf-green-ipv6)#ipv6 mroute 2003::/64 ve 10
ipv6 mroute next-hop-enable-default

You can enable an IPv6 default multicast static route to resolve other static routes.

Syntax

ipv6 mroute [next-hop-enable-default]
no ipv6 mroute [next-hop-enable-default]

Command Default

By default, the IPv6 default multicast static route is not used to resolve IPv6 multicast static route next hops.

Modes

Global configuration mode

Usage Guidelines

Before configuring an static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the `ipv6 unicast-routing` command and must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The `no` form of the command disables IPv6 multicast static route next-hop resolution through the default static route.

Examples

The following example enables the default multicast static route to resolve other static routes.

device# configure terminal
device(config)# ipv6 mroute next-hop-enable-default
ipv6 mroute next-hop-recursion
   You can resolve multicast static route destinations using recursive lookup.

Syntax
   ipv6 mroute [next-hop-recursion [number]]
   no ipv6 mroute [next-hop-recursion [number]]

Command Default
   By default, static route recursive lookup is not used to resolve IPv6 multicast static routes.

Parameters
   number
      Specifies the level of recursion for address lookup. The range is 1 through 10. If no number is specified, the default value is 3.

Modes
   Global configuration mode

Usage Guidelines
   Before configuring an IPv6 multicast static route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the ipv6 unicast-routing command, and you must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.
   The no form of the command disables IPv6 multicast static route next-hop recursion.

Examples
   The following example configures recursive static route lookup to five levels to resolve IPv6 multicast static routes.
   device# configure terminal
device(config)# ipv6 mroute next-hop-recursion 5
**ipv6 multicast-routing load-sharing rebalance**

Enables or disables the rebalance of the load-sharing among ECMP IPv6 paths.

**Syntax**

```
ipv6 multicast-routing load-sharing [ rebalance ]
```

```
no ipv6 multicast-routing load-sharing [ rebalance ]
```

**Parameters**

- `rebalance`
  
  Specifies that the ECMP load-sharing will be rebalanced for the interface on which the `rebalance` keyword is configured.

**Modes**

- Interface configuration mode

**Examples**

To configure IPv6 Multicast ECMP, use this command in the configuration mode.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ipv6 multicast-routing load-sharing
```

To disable load distribution among ECMP IP paths use the `no` form of the command.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# no ipv6 multicast-routing load-sharing
```

The following example configures rebalancing of the load distribution among ECMP IP paths.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ipv6 multicast-routing load-sharing rebalance
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was added to enable or disable the rebalance of the load-sharing among ECMP paths.</td>
</tr>
</tbody>
</table>
**ipv6 nd proxy**

Configures a single IPv6 subnet prefix to support multiple physical links in IPv6 Neighbor Discovery.

**Syntax**

```
ipv6 nd proxy
no ipv6 nd proxy
```

**Command Default**

This feature is disabled.

**Modes**

The `ipv6 nd proxy` is configurable under the global configuration mode.

**Usage Guidelines**

The IPv6 ND proxy command turns on the IPv6 ND proxy capability for the node, and is run at the configuration level.

Use the `no` form of this command to remove the ND proxy configuration.

Per RFC 4389, ND proxy can be used to bridge multiple links into a single entity to simplify management, as there is no need to allocate subnet numbers to the different networks. This can help alleviate the need to configure NAT in IPv6 networks.

**NOTE**

This is an IETF Experimental Protocol. It is the responsibility of the user to ensure that appropriate network-layer support is provided.

The following limitations apply:

- The `ipv6 nd proxy` is not supported over v6 tunnel interface.
- The `ipv6 nd proxy` programs the RACL to force the Unicast NS, sent during neighbor refresh, to the CPU for processing as proxy NS.
- The `ipv6 nd proxy` is currently supported for NS and NA messages and are not supported for other ND messages like RS, RA and redirect message.
- The `ipv6 nd proxy` is not supported for the IPsec tunnels and on MCT.

**Examples**

To enable the IPv6 ND proxy feature for the node:

```
R2>en
No password has been assigned yet...
R2#conf t
R2(config)# ipv6 nd proxy
R2(config)#
```
ipv6 nd ra-dns-server

Advertises the recursive Domain Name System (DNS) server address and the lifetime multiplier information to IPv6 hosts in the Router Advertisement (RA) message.

Syntax

ipv6 nd ra-dns-server ipv6-address [ lifetime-multiplier decimal ]

no ipv6 nd ra-dns-server ipv6-address [ lifetime-multiplier decimal ]

Command Default

By default, the recursive DNS server address and the lifetime multiplier information is not configured.

Parameters

ipv6-address

Specifies the global IPv6 address of the DNS server.

lifetime-multiplier decimal

Specifies the percentage value of the maximum router advertisement interval. The maximum router advertisement interval is the maximum time that can be allowed between sending unsolicited RA messages for DNS name resolution. The lifetime-multiplier decimal value is calculated as a percentage of the RA lifetime. The maximum router advertisement interval percentage range is 100 percent through 200 percent and the default value is 200 percent.

Modes

Global configuration mode.

Interface configuration mode.

Usage Guidelines

You can configure a maximum of four recursive DNS server addresses and corresponding lifetime multiplier values at a given instance.

no

NOTE

The `ipv6 nd ra-dns-server` command at the interface configuration level takes precedence over global configuration. In other words, if at least one DNS server address is configured on an interface, it will override other DNS server address configurations at the global configuration.

Examples

The following examples configure the recursive DNS address for a lifetime-multiplier value of 200.

device(config)# ipv6 nd ra-dns-server 2001:DC8:200::3 lifetime 200
device(config-if-e10000-1/10)# ipv6 nd ra-dns-server 2001:DC8:200::3 lifetime 200
ipv6 nd ra-domain-name

Configures the domain name of the Domain Name System (DNS) suffix and the lifetime multiplier information to IPv6 hosts in the Router Advertisement (RA) message. The no form of this command disables the advertisement of the specified domain name of DNS suffix in the RA message.

Syntax

ipv6 nd ra-domain-name string [ lifetime-multiplier decimal ]

no ipv6 nd ra-domain-name string [ lifetime-multiplier decimal ]

Parameters

- **string**: Specifies the domain name of the DNS suffix.
- **lifetime-multiplier decimal**: Specifies the percentage value of maximum router advertisement interval. The maximum router advertisement interval is the maximum time that can be allowed between sending unsolicited RA messages for DNS name resolution. The lifetime-multiplier decimal value is calculated as percentage of the RA lifetime. The maximum router advertisement interval percentage range is 100 through 200% and the default value is 200%.

Modes

- Global configuration mode.
- Interface configuration mode.

Usage Guidelines

You can configure a maximum of four different domain names of DNS suffix and corresponding lifetime multiplier values at a given instance.

The domain name of a DNS suffix at the global configuration level is used on all IPv6 routed interfaces that do not have a domain name of DNS suffix configured on them.

**NOTE**

The ipv6 nd ra-domain-name command at the interface configuration takes precedence over global configuration. In other words, if at least one DNS server address is configured on an interface, it will override other DNS server address configurations at the global configuration.

Examples

The following examples configure the domain names of a DNS suffix for a lifetime-multiplier value of 200.

```
device (config)# ipv6 nd ra-domain-name brocade.com lifetime 200
device (config-if-e10000-1/10)# ipv6 nd ra-domain-name brocade.com lifetime 200
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**ipv6 ospf active**
Sets a specific OSPFv3 interface to active.

**Syntax**
```
ipv6 ospf active
```

**Modes**
Interface subtype configuration mode

**Usage Guidelines**
Use the `ipv6 ospf active` command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPFv3 control packets.

**Examples**
The following example sets a specific OSPFv3 Ethernet interface to active.
```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf active
```
**ipv6 ospf area**

Enables OSPFv3 on an interface.

**Syntax**

```
ipv6 ospf area area-id | ipv6-addr
no ipv6 ospf area
```

**Command Default**

OSPFv3 is disabled.

**Parameters**

- `area-id`
  Area address in dotted decimal or decimal format.

- `ipv6-addr`
  IPv6 address.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

This command enables an OSPFv3 area on the interface to which you are connected.

The `no` form of the command disables OSPFv3 on this interface.

**Examples**

The following example enables a configured OSPFv3 area named 0 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
```
**ipv6 ospf authentication ipsec**

Specifies IP security (IPsec) as the authentication type for an OSPFv3 interface.

**Syntax**

```
ipv6 ospf authentication ipsec key-add-remove-interval interval
no ipv6 ospf authentication ipsec key-add-remove-interval interval
```

**Command Default**

Disabled.

**Parameters**

- **key-add-remove-interval interval**
  
  Specifies the OSPFv3 authentication key add-remove interval. Valid values range from decimal numbers 0 through 14400. The default is 300.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

The **no** form of the command removes IPsec authentication from the interface.

**Examples**

The following example enables IPsec on a specified OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec
```

The following example sets the OSPFv3 authentication key add-remove interval to 480.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec key-add-remove-interval 480
```
ipv6 ospf authentication ipsec disable

Disables IP security (IPsec) services on an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec disable

no ipv6 ospf authentication ipsec disable

Command Default

Authentication is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to disable IPsec if it is enabled on the interface. Packets that are sent out will not be IPSec encapsulated and the received packets which are IPSec encapsulated will be dropped.

The no form of the command re-enables IPSec on the interface if IPsec is already configured on the interface.

Examples

The following example disables IPsec on a specific OSPFv3 interface where IPsec is already enabled.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec disable
ipv6 ospf authentication ipsec spi

Specifies the IP security (IPsec) security policy index (SPI) value for an OSPFv3 interface.

Syntax

```
ipv6 ospf authentication ipsec spi value esp sha1 key [ no-encrypt ] key
no ipv6 ospf authentication spi
```

Command Default

Authentication is disabled.

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

Parameters

- **ipsec**
  Specifies IPsec as the authentication protocol.
- **spi**
  Specifies the Security Policy Index (SPI).
- **value**
  Specifies the SPI value. Valid values range from decimal numbers 256 through 4294967295. The near-end and far-end values must be the same.
- **esp**
  Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security. This is the only option currently available.
- **sha1**
  Enables Hashed Message Authentication Code (HMAC) Secure Hash Algorithm 1 (SHA-1) authentication.
- **key**
  Number used in the calculation of the message digest. The 40 hexadecimal character key is stored in encrypted format by default.
- **no-encrypt**
  The 40-character key is not encrypted upon either its entry or its display.
- **key**
  The 40 hexadecimal character key.

Modes

Interface subtype configuration mode
**Usage Guidelines**

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

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

To change an existing key, you must specify a different SPI value to that of the value already configured. The `no` form of the command removes the SPI value from the interface.

**Examples**

The following example enables ESP and HMAC-SHA-1 on a specified OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf area 0
device(config-if-e1000/1/1)# ipv6 ospf authentication ipsec spi 512 esp sha1 abcef12345678901234fedcba098765432109876
```
**ipv6 ospf bfd**

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv3 interface.

**Syntax**

```
ipv6 ospf bfd disable
no ipv6 ospf bfd
```

**Command Default**

BFD is disabled by default.

**Parameters**

- **disable**
  
  Disables BFD on the OSPFv3 interface.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

BFD sessions are initiated if BFD is also enabled globally using the `bfd all-interfaces` command in OSPFv3 router configuration mode. If BFD is disabled using the `no bfd all-interfaces` command in OSPFv3 router configuration mode, BFD sessions on specific interfaces are deregistered.

The `no` form of the command removes all BFD sessions from a specified interface.

**Examples**

The following example enables BFD on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf bfd
```

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

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf bfd disable
```
**ipv6 ospf cost**

Configures cost for a specific OSPFv3 interface.

**Syntax**

```
ipv6 ospf cost value
no ipv6 ospf cost
```

**Command Default**

Cost value is 1.

**Parameters**

- `value`
  
  Cost value. Valid values range from 1 through 65535. The default is 1.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

Use this command to set or reset the OSPFv3 cost on the interface. If the cost is not configured with this command, OSPFv3 calculates the value from the reference and interface bandwidths.

For more information, refer to the `auto-cost reference-bandwidth` command.

The `no` form of the command disables the configured cost.

**Examples**

The following example sets the cost to 620 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf cost 620
```
ipv6 ospf dead-interval

Specifies the time period for which a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ipv6 ospf dead-interval interval
no ipv6 ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 65535 seconds. The default is 40.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the ipv6 ospf hello-interval command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is $\frac{1}{4}$ times that of the dead interval.

The running-config command displays only explicitly configured values of the hello interval, which means that a value that was automatically changed as the result of a dead-interval change is not displayed.

The no form of the command restores the default value.

Examples

The following example sets the dead interval to 80 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf dead-interval 80
```
ipv6 ospf hello-interval

Sets the length of time between the transmission of hello packets that an interface sends to neighbor routers.

Syntax
ipv6 ospf hello-interval interval
no ipv6 ospf hello-interval

Command Default
The length of time between the transmission of hello packets is set to 10 seconds.

Parameters
interval
Hello interval in seconds. Valid values range from 1 through 65535 seconds. The default is 10.

Modes
Interface subtype configuration mode

Usage Guidelines
If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello interval, unless the dead interval is also explicitly configured using the ipv6 ospf dead-interval command.

The recommended setting is that:
• The dead interval is four times that of the hello interval.
• The hello interval is ¼ times that of the dead interval.

The running-config command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello interval change is not displayed.

The no form of the command restores the default value.

Examples
The following example sets the hello interval to 20 on a specific OSPFv3 Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 ospf hello-interval 20
**ipv6 ospf hello-jitter**

Sets the allowed jitter between HELLO packets.

**Syntax**

```
ipv6 ospf hello-jitter interval
no ipv6 ospf hello-jitter
```

**Parameters**

- **jitter**
  
  Allowed interval between hello packets. Valid values range from 1 through 50 percent (%).

**Modes**

- Interface subtype configuration mode

**Usage Guidelines**

The hello interval can vary from the configured hello-interval to a maximum of percentage value of configured jitter.

**Examples**

The following example sets the hello jitter to 20 on a specific OSPFv3 Ethernet interface.

```bash
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf hello-jitter 20
```
**ipv6 ospf instance**

Specifies the number of OSPFv3 instances running on an interface.

**Syntax**

```
ipv6 ospf instance instanceID
no ipv6 ospf instance
```

**Parameters**

```
instanceID
```

Instance identification number. Valid values range from 0 through 255.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

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

**Examples**

The following example sets the number of IPv6 OSPF instances to 35 on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf instance 35
```
**ipv6 ospf mtu-ignore**

Enables or disables maximum transmission unit (MTU) match checking.

**Syntax**

```
ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore
```

**Command Default**

Enabled.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

In default operation, the IP MTU on both sides of an OSPFv3 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The `no` form of the command disables MTU-match checking on a specific interface.

**Examples**

The following example disables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# no ipv6 ospf mtu-ignore
```

The following example enables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf mtu-ignore
```
ipv6 ospf network

Configures network type.

Syntax

ipv6 ospf network { broadcast | point-to-point }

no ipv6 ospf network

Command Default

Network type is broadcast for Ethernet and VE interfaces. Network type is point-to-point for tunnel and GRE interfaces.

Parameters

- **broadcast**
  Network type is broadcast, such as Ethernet.

- **point-to-point**
  Network type is point-to-point.

Modes

- Interface subtype configuration mode

Usage Guidelines

Point-to-point can support unnumbered links, which requires less processing by OSPFv3.

The **no** form of the command removes the network-type configuration.

**NOTE**

The network type non-broadcast is not supported at this time.

Examples

The following example configures an OSPFv3 point-to-point link on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf network point-to-point
```

The following example configures an OSPFv3 broadcast link on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf network broadcast
```
**ipv6 ospf passive**

Sets a specific OSPFv3 interface to passive.

**Syntax**

```
ipv6 ospf passive
no ipv6 ospf passive
```

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

The `ipv6 ospf passive` command disables transmission of OSPFv3 control packets on that interface. OSPFv3 control packets received on a passive interface are discarded.

The `no` form of the command sets an interface back to active.

**Examples**

The following example sets a specific OSPFv3 Ethernet interface to passive.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf passive
```
**ipv6 ospf priority**

Configures priority for designated router (DR) election and backup designated routers (BDRs) on the interface you are connected to.

**Syntax**

```plaintext
ipv6 ospf priority value
no ipv6 ospf priority
```

**Command Default**

The value is set to 1.

**Parameters**

```plaintext
value
```

Priority value. Valid values range from 0 through 255. The default is 1.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

The OSPFv3 router assigned the highest priority becomes the designated router, and the OSPFv3 router with the second-highest priority becomes the backup router.

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

**Examples**

The following example sets a priority of 4 for the OSPFv3 router that is connected to an OSPFv3 Ethernet interface.

```plaintext
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf priority 4
```
**ipv6 ospf retransmit-interval**

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

**Syntax**

```
ipv6 ospf retransmit-interval interval
no ipv6 ospf retransmit-interval
```

**Command Default**

The interval is 5 seconds.

**Parameters**

`interval`

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds. The default is 5.

**Modes**

Interface subtype configuration mode

**Usage Guidelines**

The `no` form of the command resets the retransmit interval to its default.

**Examples**

The following example sets the retransmit interval to 8 for all OSPFv3 devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf retransmit-interval 8
```
**ipv6 ospf suppress-linklsa**

Suppresses link LSA advertisements.

**Syntax**

```cpp
ipv6 ospf suppress-linklsa
no ipv6 ospf suppress-linklsa
```

**Modes**

Interface subtype configuration mode

**Examples**

The following example suppresses link LSAs from being advertised on devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf suppress-linklsa
```
ipv6 ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv3 to send link-state update packets on the interface to which you are connected.

Syntax

ipv6 ospf transmit-delay value
no ipv6 ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The no form of the command restores the default value.

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv3 Ethernet interface.

device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000/1/1)# ipv6 ospf transmit-delay 25
**ipv6 rate-limit hoplimit-expired-to-cpu**

Applies rate-limit option on IPv6 hop-limit packets, if the hop-limit count is less than or equal to one.

**Syntax**

```
ipv6 rate-limit hoplimit-expired-to-cpu rate-limit policy
no ipv6 rate-limit hoplimit-expired-to-cpu rate-limit policy
```

**Command Default**

By default, the no rate-limit option is applied to IPv6 hop-limit packets, if the hop-limit count is less than or equal to one.

**Parameters**

- `rate-limit policy`
  
  Name of the policy-map.

**Modes**

Global configuration mode.

**Usage Guidelines**

Create CPU bound rate-limit policy map before applying rate-limiting for hop-limit packets.

**NOTE**

The following warning message is displayed if only some of the cards are supported and few are not supported.

```
Warning: rate-limit config for protocol "hoplimit-expired-to-cpu" is not supported on module 1, 3
```

**NOTE**

The following warning message is displayed if none of the cards are supported.

```
Warning: rate-limit config for protocol "hoplimit-expired-to-cpu" is not supported on available modules.
It is only supported on GEN-2 and later modules.
```

The no form of the command disables rate-limit option on IPv6 hop-limit packets.

**Examples**

The following example explains how to apply a rate-limit policy for IPv6 hop-limit packets.

```
device(config)# ipv6 rate-limit hoplimit-expired-to-cpu policy-map save-cpu-policy
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipv6 receive access-list

Configures an IPv6 access-control list as an IPv6 receive access-control list (rACL).

Syntax

ipv6 receive access-list acl-name sequence seq-num [ policy-map policy-map-name [ strict-acl ] ]

no ipv6 receive access-list acl-name sequence seq-num [ policy-map policy-map-name [ strict-acl ] ]

Parameters

- **acl-name**: Specifies the name of the access-control list to apply to all interfaces within the default VRF, for all CPU-bound traffic. The maximum length of the access-control list name is 256 characters.

- **sequence seq-num**: Defines the sequence number of the access-control list being applied as a rACL. IPv6 rACL commands are applied in the order of the lowest to the highest sequence numbers. The range of values is from 1 through 50.

- **policy-map policy-map-name**: Specifies the name of a policy map. When the policy-map option is specified, traffic matching the “permit” clause of the specified IPv6 ACL is rate-limited as defined in the policy map and IPv6 traffic matching the “deny” clause in the IPv6 ACL is permitted without any rate limiting.

- **strict-acl**: Specifies that traffic matching the “permit” clause of the specified IPv6 ACL is rate-limited as defined in the policy map and IPv6 traffic matching the “deny” clause in the IPv6 ACL is dropped in the hardware.

Modes

- Global configuration mode

Usage Guidelines

The rACL works like a regular ACL where IPv6 traffic matching the “permit” clause specified in the IPv6 ACL is permitted, and IPv6 traffic matching the “deny” clause in the IPv6 ACL is dropped in hardware.

The **no** form of the basic command removes the rACL.

The **no** form of the command with both policy-map and strict-acl options specified, removes the strict-acl option: the rACL with policy-map remains and traffic matching “deny” clauses starts passing to the CPU.

Examples

The following example configures an IPv6 rACL to apply the ACL “b1” with a sequence number of “15” to all interfaces within the default VRF, for all CPU-bound traffic.

device(config)# ipv6 receive access-list b1 sequence 15

The following example configures an IPv6 rACL with a policy map “m1”. The rACL applies the ACL “b1” with a sequence number of “15” to all interfaces within the default VRF, for all CPU-bound traffic. Traffic matching the permit clause of the “b1” ACL is rate-limited as defined in in the policy map “m1” and traffic matching the “deny” clause in “b1” ACL is permitted without any rate limiting.

device(config)# ipv6 receive access-list b1 sequence 15 policy map m1
The following example removes the **strict-acl** option so that traffic matching “deny” clauses starts passing to the CPU: the rACL with the policy map "m1" remains.

device(config)# no ipv6 receive access-list b1 sequence 15 policy-map m1 strict-acl

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was modified to support named rACLs.</td>
</tr>
</tbody>
</table>
**ipv6 receive access-list enable-deny-logging**

Generates logs for a specific interface that contain IPv6 packets that are denied as a result of a receive access-control list (rACL).

**Syntax**

```
ipv6 receive access-list enable-deny-logging [ hw-drop ]
no ipv6 receive access-list enable-deny-logging [ hw-drop ]
```

**Command Default**

Logs are not generated for IPv6 packets that are denied by an rACL.

**Parameters**

- **hw-drop**
  
  Drops the denied IPv6 packets in hardware.

**Modes**

Interface configuration mode

**Usage Guidelines**

By default, any IPv6 packets received on an interface that are denied by an rACL are discarded by the software. To avoid high CPU usage when you enable the log generation of denied IPv6 packets, configure the optional `hw-drop` keyword to drop the IPv6 packets in the hardware after the log is generated.

The no form of this command disables the log generation.

**NOTE**

The `ipv6 receive access-list enable-deny-logging` command is supported only on Brocade NetIron MLX Series devices.

**Examples**

The following example creates an rACL to deny packets and enables the generation of IPv6 packet logging on Ethernet interface 1/1.

```
device# configure terminal
device(config)# ipv6 receive access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 receive access-list deny-log in
device(config-if-e1000-1/1)# ipv6 receive access-list enable-deny-logging
```
The following example creates an rACL to deny packets, enables the generation of IPv6 packet logging on Ethernet interface 1/1 and drops the packets in hardware.

device# configure terminal
device(config)# ipv6 receive access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 receive access-list deny-log in
device(config-if-e1000-1/1)# ipv6 receive access-list enable-deny-logging hw-drop

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipv6 receive deactivate-acl-all

Deactivates the IPv6 receive access-control list (rACL) configuration and removes all rules from Content Addressable Memory (CAM). The no form of this command re-activates the rACL configuration.

Syntax

ipv6 receive deactivate-acl-all
no ipv6 receive deactivate-acl-all

Modes

Global configuration mode.

Usage Guidelines

Use the write memory command to save this configuration permanently and to prevent ACL binding to CAM after reload.

The no version of the command removes the configured deactivate option and sets it to default.

Examples

The following example deactivates the IPv6 rACL configuration.
device(config)# ipv6 receive deactivate-acl-all

The following example re-activates the IPv6 rACL configuration.
device(config)# no ipv6 receive deactivate-acl-all

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipv6 receive delete-acl-all

Deletes IPv6 receive access-control list (rACL) rules from the system.

Syntax

ipv6 receive delete-acl-all

Modes

Global configuration mode.

Usage Guidelines

You must confirm that you wish to proceed with the deletion. Enter ‘y’ or ‘n’ in response to the prompt “Are you sure?.”

Examples

The following example deletes all IPv6 rACL rules from the system.

device(config)# ipv6 receive delete-acl-all
This command deletes all IP Receive ACLs from system.
Are you sure? (enter 'y' or 'n'): y

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipv6 receive rebind-acl-all

Rebinds an IPv6 receive access-control list (rACL).

Syntax

ipv6 receive rebind-acl-all

Modes

Global configuration mode.

Usage Guidelines

When access list rules are modified or a policy map associated with a rACL is changed, an explicit rebind must be performed to propagate the changes to the interfaces.

Examples

The following example rebinds an IPv6 rACL.

device(config)# ipv6 receive rebind-acl-all

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipv6 route

Configures a static IPv6 route for an interface.

Syntax

```
ipv6 route dest-ipv6-prefix/prefix-length [ ve ve-id | ipv6_tnl tunnel-id | 6to4_tnl tunnel_id | link-local-next-hop-ipv6-address ] [ metric ] [ distance number ] [ tag tag-number ] [ name string ]
```

```
ipv6 route dest-ipv6-prefix/prefix-length [ ethernet slot/port [ link-local-next-hop-ipv6-address ] ] [ metric ] [ distance number ] [ tag tag-number ] [ name string ]
```

```
ipv6 route ipv6-prefix/prefix-length next-hop-vrf vrf_name next-hop-ipv6-address [ metric ] [ distance number ] [ tag tag-number ]
```

```
ipv6 route dest-ipv6-prefix/prefix-length null0 [ metric ] [ distance number ] [ tag tag-number ]
```

```
no ipv6 route dest-ipv6-prefix|prefix-length [ ve ve-id | ipv6_tnl tunnel-id | 6to4_tnl tunnel_id | link-local-next-hop-ipv6-address ] [ metric ] [ distance number ] [ tag tag-number ] [ name string ]
```

```
no ipv6 route dest-ipv6-prefix|prefix-length [ ethernet slot/port [ link-local-next-hop-ipv6-address ] ] [ metric ] [ distance number ] [ tag tag-number ] [ name string ]
```

```
no ipv6 route ipv6-prefix|prefix-length next-hop-vrf vrf_name next-hop-ipv6-address [ metric ] [ distance number ] [ tag tag-number ]
```

```
no ipv6 route dest-ipv6-prefix|prefix-length null0 [ metric ] [ distance number ] [ tag tag-number ]
```

Command Default

An IPv6 static route is not configured.

Parameters

```
dest-ipv6-prefix
```

Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

```
prefix-length
```

A decimal value specifying the length of the IPv6 prefix.

```
next-hop-ipv6-address
```

IPv6 address of the next-hop gateway.

```
link-local-next-hop-ipv6-address
```

IPv6 address of the link-local next-hop gateway.

```
next-hop-vrf vrf_name next-hop-ipv6-address
```

Specifies a VRF instance and a next-hop IPv6 address.

```
null0
```

Causes packets to the selected destination to be dropped by shunting them to the "null0" interface. (This is the only available option.)

```
ethternet slot/port
```

Specifies the Ethernet slot or port.
ve ve-id
    Specifies the virtual Ethernet (VE) interface VE ID.

6to4_tnl tunnel-id
    Specifies IPv6 to IPv4 tunnel number to be used as next hop.

ipv6_tnl tunnel-id
    Specifies IPv6 tunnel to be used as next hop.

ame string
    Optional name (ASCII string) assigned to the route

metric
    Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance number
    Specifies an administrative distance. The range is from 1 through 255. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route.

tag
    Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

tag-number
    A number from 0 through 4294967295. The default is 0.

Modes
    Global configuration mode

    VRF configuration mode

Usage Guidelines
    The no form of the command removes the IPv6 static route. If the route is named, the no command must be used twice, the first time to remove the name and the second time to remove the route.
Examples

To configure the IPv6 ND proxy static route by specifying the destination prefix and the outgoing interface:

\[\text{NOTE}\]
As per the topology mentioned in the packet flow, if the IPv6 ND proxy is configured on R2, then this static route can be configured on R1 with the destination prefix being 2002::/64. The static route can also be configured with outgoing interface as ve, such as ve 10.

```
R1(config)#
R1(config)# ipv6 route 2002::/64 ethernet 1/1

R1(config)#
R1(config)# ipv6 route 2003::/64 ve 10

R1(config)# vrf green
R1(config-vrf-green)# address-family ipv6
R1(config-vrf-green-ipv6)# ipv6 route 2002::/64 eth 1/1

R1(config)# vrf green
R1(config-vrf-green)# address-family ipv6
R1(config-vrf-green-ipv6)# ipv6 route 2003::/64 ve 10
```

To show the running-config (with truncated output showing only the static route):

```
R1(config)# ipv6 route 2002::/64 ethernet 1/1
R1(config)# ipv6 route 2003::/64 ve 10

vrf green
rd 66:66
address-family ipv6
ipv6 route 2002::/64 ethernet 1/1
ipv6 route 2003::/64 ve 10
R1(config)# exit-vrf
```
ipv6 route bfd

Enables Bidirectional Forwarding Detection (BFD) monitoring for an IPv6 static route.

Syntax

ipv6 route dest-ipv6-prefix/prefix-length next-hop-ipv6-address bfd

ipv6 route dest-ipv6-prefix/prefix-length next-hop-ipv6-address bfd [ metric | distance number | name name | tag number ]

Command Default

BFD monitoring for an IPv6 static route is not enabled.

Parameters

dest-ipv6-prefix

Specifies the destination IPv6 prefix in hexadecimal with 16-bit values between colons.

prefix-length

A decimal value specifying the length of the IPv6 prefix.

next-hop-ipv6-address

Specifies the IPv6 address of the next hop.

metric

Specifies the cost metric of the route. Valid values range from 1 through 16. The default is 1.

distance number

Specifies the administrative distance of the route. Valid values range from 1 through 255. The default is 1.

name name

Specifies the name of the route in ASCII characters.

tag number

Specifies the tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

Usage Guidelines

The no form of the command removes BFD monitoring from the static route.

Examples

The following example enables BFD route monitoring on an IPv6 static route and sets the cost metric of the route to 10.

device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd 10
The following example enables BFD route monitoring on an IPv6 static route and sets the administrative distance of the route to 55.

```
device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd distance 55
```

The following example enables BFD route monitoring on an IPv6 static route and sets the name of the route to "routered".

```
device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd name routered
```

The following example enables BFD route monitoring on an IPv6 static route and sets the tag value of the route to 100.

```
device# configure terminal
device(config)# ipv6 route 2001:db8::0/32 2001:db:0:ee44::1 bfd tag 100
```
ipv6 route next-hop

Enables the Brocade device to use routes from a specified protocol to resolve a configured IPv6 static route.

Syntax

ipv6 route next-hop { bgp | isis | ospf | rip }
no ipv6 route next-hop { bgp | isis | ospf | rip }

Command Default
The Brocade device is not enabled to use routes from a specified protocol to resolve a configured IPv6 static route.

Parameters

bgp
  Configures the device to use iBGP and eBGP routes to resolve static routes.

isis
  Configures the device to use ISIS to resolve static routes.

ospf
  Configures the device to use OSPF routes to resolve static routes.

rip
  Configures the device to use RIP routes to resolve static routes.

Modes
Global configuration mode

Usage Guidelines
Before configuring a static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the ipv6 unicast-routing command and enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The no form of the command disables IPv6 static route resolution through the designated protocol.

Examples
The following example configures the device to use OSPF protocol to resolve IPv6 static routes.

device# configure terminal
device(config)# ipv6 route next-hop ospf
ipv6 route next-hop-enable-default

You can enable the IPv6 default static route to resolve other static routes.

Syntax

ipv6 route [ next-hop-enable-default ]
no ipv6 route [ next-hop-enable-default ]

Command Default

By default, the IPv6 default static route is not used to resolve IPv6 static route next hops.

Modes

Global configuration mode

Usage Guidelines

Before configuring a static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the ipv6 unicast-routing command and must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The no form of the command disables IPv6 static route next-hop resolution through the default static route.

Examples

The following example enables the default static route to resolve other static routes.

device# configure terminal
device(config)# ipv6 route next-hop-enable-default
**ipv6 next-hop-recursion**

You can resolve static route destinations using recursive lookup.

**Syntax**

```plaintext
ipv6 route [ next-hop-recursion [ number ] ]
no ipv6 route [ next-hop-recursion [ number ] ]
```

**Command Default**

By default, static route recursive lookup is not used to resolve IPv6 static routes.

**Parameters**

`number`

Specifies the level of recursion for address lookup. The range is 1 through 10. If no number is specified, the default value is 3.

**Modes**

Global configuration mode

**Usage Guidelines**

Before configuring a static IPv6 route, you must enable the forwarding of IPv6 traffic on the Layer 3 switch using the `ipv6 unicast-routing` command, and you must enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface.

The `no` form of the command disables IPv6 static route next-hop recursion.

**Examples**

The following example configures recursive static route lookup to five levels to resolve IPv6 static routes.

```plaintext
device# configure terminal
device(config)# ipv6 route next-hop-recursion 5
```
ipv6 route static-bfd

Configures Bidirectional Forwarding Detection (BFD) session parameters for IPv6 static routes.

Syntax

```
ipv6 route [ vrf vrf-name ] static-bfd dest-ipv6-address source-ipv6-address [ interval transmit-time min-rx receive-time multiplier number ]
no ipv6 route [ vrf vrf-name ] static-bfd dest-ipv6-address source-ipv6-address
```

Command Default

BFD is not configured for an IPv6 static route.

Parameters

- **vrf vrf-name**
  Specifies the name of a VRF instance.

- **dest-ipv6-address**
  Specifies the destination IPv6 address.

- **source-ipv6-address**
  Specifies the source IPv6 address.

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

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

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

Modes

Global configuration mode

Usage Guidelines

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

For single-hop static BFD sessions, timeout values are optional because all required information is available from the outgoing interface. For multi-hop BFD sessions, if the configured `interval` and `min-rx` parameters conflict with those of an existing BGP session, the lower values are used.
If you configure a neighbor IPv6 address and a source IPv6 address that already exist in BFD, BFD overwrites the existing interval values and multiplier for the IPv6 addresses with the new values on behalf of the static module.

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

The **no** form of the command removes the configured BFD IPv6 static route.

**Examples**

The following example configures a BFD session on an IPv6 static route.

```bash
device# configure terminal
device(config)# ipv6 route static-bfd fe80::a fe80::b interval 100 min-rx 100 multiplier 10
```
**ipv6 router ospf**

Enables and configures the Open Shortest Path First version 3 (OSPFv3) routing protocol.

**Syntax**
```
ipv6 router ospf [vrf name]
no ipv6 router ospf
```

**Command Default**
This command is disabled by default.

**Parameters**
```
vrf name
```
Specifies a nondefault VRF.

**Modes**
Global configuration mode

**Usage Guidelines**
If you save the configuration to the startup-config file after disabling OSPFv3, all OSPFv3 configuration information is removed from the startup-config file.

Use this command to enable the OSPFv3 routing protocol and enter OSPFv3 router or OSPFv3 router VRF configuration mode. OSPFv3 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

The **no** form of the command deletes all current OSPFv3 configurations and blocks any further OSPFv3 configuration.

**Examples**
The following example enables OSPFv3 on a default VRF and enters OSPFv3 router configuration mode.
```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)#
```
ipv6 router vrrp


Syntax

ipv6 router vrrp

no ipv6 router vrrp

Command Default

IPv6 VRRP is not globally enabled.

Modes

Global configuration mode

Usage Guidelines

After globally enabling IPv6 VRRP, the command prompt does not change. Nearly all subsequent IPv6 VRRP configuration is performed at the interface level, but IPv6 VRRP must be enabled globally before configuring IPv6 VRRP instances.

The no form of the command disables VRRP globally.

Examples

The following example enables IPv6 VRRP globally and enters interface configuration mode to allow you to enter more VRRP configuration.

device# configure terminal
device(config)# ipv6 router vrrp
device(config-ipv6-vrrp-router)# interface ethernet 1/4
device(config-if-e1000-1/4)# ipv6 address fd3b::3/64
device(config-if-e1000-1/4)# ipv6 vrrp vrid 2
device(config-if-e1000-1/4-vrid-2)# backup priority 100
device(config-if-e1000-1/4-vrid-2)# version 3
device(config-if-e1000-1/4-vrid-2)# advertise backup
device(config-if-e1000-1/4-vrid-2)# ipv6-address fe80::768e:f8ff:fe2a:0099
device(config-if-e1000-1/4-vrid-2)# ipv6-address fd3b::2
device(config-if-e1000-1/4-vrid-2)# activate
**ipv6 router vrrp-extended**


**Syntax**

- ipv6 router vrrp-extended
- no ipv6 router vrrp-extended

**Command Default**

VRRP-E is not globally enabled.

**Modes**

Global configuration mode

**Usage Guidelines**

After globally enabling IPv6 VRRP-E, nearly all subsequent IPv6 VRRP-E configuration is performed at the interface level. If IPv6 VRRP-E is not globally enabled, you will see an error message when configuring IPv6 VRRP-E instances.

The `no` form of the command disables VRRP-E globally.

**Examples**

The following example enables IPv6 VRRP-E globally and enters interface configuration mode for subsequent IPv6 VRRP-E configuration.

```
device# configure terminal
device(config)# ipv6 router vrrp-extended
device(config-ipv6-vrrpe-router)# interface ethernet 1/5
```
ipv6 traffic-filter
Applies an IPv6 ACL to incoming or outgoing traffic on an interface.

Syntax
ipv6 traffic-filter acl-name { in | out }
no ipv6 traffic-filter acl-name { in | out }

Command Default
No IPv6 ACL is applied to the interface.

Parameters
acl-name
Specifies the name of the IPv6 ACL.
in
Applies the ACL to incoming IPv6 packets on the interface.
out
Applies the ACL to outgoing IPv6 packets on the interface.

Modes
Interface subtype configuration modes

Usage Guidelines
To remove an ACL from an interface, use the no form of this command.

Examples
The following example creates an IPv6 ACL, defines within it a rule that blocks all Telnet traffic received from IPv6 host 2000:2382:e0bb::2, and applies the ACL to port 1/1.

device# configure terminal
device(config)# ipv6 access-list fdry
device(config-ipv6-access-list-fdry)# deny tcp host 2000:2382:e0bb::2 any eq telnet
device(config-ipv6-access-list-fdry)# permit ipv6 any any
device(config-ipv6-access-list-fdry)# exit
device(config)# interface ethernet 1/1
device(config-if-1/1)# ipv6 traffic-filter fdry in
device(config-if-1/1)# exit
device(config)# write memory
The first phase of the following example creates an IPv6 ACL, and defines the following rules within:

- Permit ICMP traffic from hosts in the 2000:2383:e0bb::x network to hosts in the 2001:3782::x network.
- Deny all IPv6 traffic from host 2000:2383:e0ac::2 to host 2000:2383:e0aa:0::24.
- Deny all UDP traffic.
- Permit all packets that are not explicitly denied by the other entries. (Without this entry, the ACL denies all incoming or outgoing IPv6 traffic on the ports to which the ACL is assigned.)

```plaintext
device(config)# ipv6 access-list netw
device(config-ipv6-access-list-netw)# permit icmp 2000:2383:e0bb::/64 2001:3782::/64
device(config-ipv6-access-list-netw)# deny ipv6 host 2000:2383:e0ac::2 host 2000:2383:e0aa:0::24
device(config-ipv6-access-list-netw)# deny udp any any
device(config-ipv6-access-list-netw)# permit ipv6 any any
device(config-ipv6-access-list-netw)# exit
```

The second phase of the example applies the ACL to both incoming and outgoing traffic on port 1/2 and to incoming traffic on port 4/3.

```plaintext
device(config)# interface ethernet 1/2
device(config-if-1/2)# ipv6 traffic-filter netw in
device(config-if-1/2)# ipv6 traffic-filter netw out
device(config-if-1/2)# exit
device(config)# interface ethernet 4/3
device(config-if-4/3)# ipv6 traffic-filter netw in
device(config-if-4/3)# exit
device(config)# write memory
```
**ipv6 traffic-filter enable-deny-logging**

Generates logs for a specific interface that contain IPv6 packets that are denied as a result of an access-control list (ACL).

**Syntax**

```
ipv6 traffic-filter enable-deny-logging [ hw-drop ]
no ipv6 traffic-filter enable-deny-logging [ hw-drop ]
```

**Command Default**

Logs are not generated for IPv6 packets that are denied by an ACL.

**Parameters**

- **hw-drop**
  
  Drops the denied IPv6 packets in hardware.

**Modes**

Interface configuration mode

**Usage Guidelines**

By default, any IPv6 packets received on an interface that are denied by an ACL are discarded by the software. To avoid high CPU usage when you enable the log generation of denied IPv6 packets, configure the optional `hw-drop` keyword to drop the IPv6 packets in the hardware after the log is generated.

The `no` form of this command disables the log generation of denied IPv6 packets.

**NOTE**

The `ipv6 traffic-filter enable-deny-logging` command is supported only on Brocade NetIron MLX Series devices.

**Examples**

The following example creates an ACL to deny packets and enables the generation of IPv6 packet logging on Ethernet interface 1/1.

```
device# configure terminal
device(config)# ipv6 access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 traffic-filter deny-log in
device(config-if-e1000-1/1)# ipv6 traffic-filter enable-deny-logging
```
The following example creates an ACL to deny packets, enables the generation of IPv6 packet logging on Ethernet interface 1/1 and drops the packets in hardware.

```
device# configure terminal
device(config)# ipv6 access-list deny-log
device(config-ipv6-access-list deny-log)# deny ipv6 any any log
device(config-ipv6-access-list deny-log)# exit
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# ipv6 traffic-filter deny-log in
device(config-if-e1000-1/1)# ipv6 traffic-filter enable-deny-logging hw-drop
```

**NOTE**

The command `ipv6 traffic-filter enable-deny-logging` is supported for LAG ports. If we enable the command on LAG ports, a CAM index is created only on the primary port.

The following example configures the LAG.

```
device(config)# lag  lag1 static id 1
device(config-lag-lag1)# ports Ethernet 1/1 to 1/4
device(config-lag-lag1)# primary Ethernet 1/1
device(config-lag-lag1)# deploy

device(config-if-e1000-1/1)# ipv6 traffic-filter deny-log in
device(config-if-1/1)# ipv6 traffic-filter enable-deny-logging hw-drop
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
ipv6 vrrp vrid

Configures an IPv6 Virtual Router Redundancy Protocol (VRRP) virtual router identifier (VRID).

Syntax

ipv6 vrrp vrid vrid
no ipv6 vrrp vrid vrid

Command Default

An IPv6 VRRP VRID does not exist.

Parameters

vrid

Configures a number for the IPv6 VRRP VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that IPv6 VRRP is enabled globally; otherwise, an error stating "Invalid input..." is displayed as you try to create a VRRP instance.

The no form of this command removes the IPv6 VRRP VRID from the configuration.

Examples

The following example configures IPv6 VRRP VRID 1.

device# configure terminal
device(config)# ipv6 router vrrp
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 address fd2b::2/64
device(config-if-e1000-1/5)# ipv6 vrrp vrid 2
device(config-if-e1000-1/5-vrid-2)# owner
device(config-if-e1000-1/5-vrid-2)# ipv6-address fe80::768e:f8ff:fe2a:0099
device(config-if-e1000-1/5-vrid-2)# ipv6-address fd2b::2
device(config-if-e1000-1/5-vrid-2)# activate
ipv6 vrrp-extended vrid


Syntax

ipv6 vrrp-extended vrid vrid
no ipv6 vrrp-extended vrid vrid

Command Default

An IPv6 VRRP-E VRID does not exist.

Parameters

vrid

Configures a number for the IPv6 VRRP-E VRID. The range is from 1 through 255.

Modes

Interface configuration mode

Usage Guidelines

Before configuring this command, ensure that IPv6 VRRP-E is enabled globally; otherwise, an error stating “Invalid input…” is displayed as you try to create a VRRP-E instance.

The no form of this command removes the IPv6 VRRP-E VRID from the configuration.

Examples

The following example configures IPv6 VRRP-E VRID 2.

device# configure terminal
device(config)# ipv6 router vrrp-extended
device(config-ipv6-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ipv6 address fd4b::2/64
device(config-if-e1000-1/5)# ipv6 vrrp-extended vrid 2
device(config-if-e1000-1/5-vrid-2)# backup priority 50 track-priority 10
device(config-if-e1000-1/5-vrid-2)# ipv6-address fe80::768e:f8ff:fe3a:0099
device(config-if-e1000-1/5-vrid-2)# ipv6-address fd4b::99
device(config-if-e1000-1/5-vrid-2)# activate
**isis bfd**

Enables Bidirectional Forwarding Detection (BFD) on a specific IS-IS interface.

**Syntax**

```plaintext
isis bfd disable
no isis bfd
```

**Command Default**

BFD is disabled by default.

**Parameters**

- `disable`
  
  Disables BFD on the IS-IS interface.

**Modes**

- Interface subtype configuration mode

**Usage Guidelines**

BFD sessions are initiated if BFD is enabled globally using the `bfd all-interfaces` command in IS-IS router configuration mode. If BFD is disabled using the `no bfd all-interfaces` command in IS-IS router configuration mode, BFD sessions on specific IS-IS interfaces are deregistered.

The `no` form of the command removes all BFD sessions from a IS-IS specified interface.

**Examples**

The following example enables BFD on a specific IS-IS Ethernet interface.

```plaintext
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis bfd
```

The following example disables BFD on a specific IS-IS Ethernet interface.

```plaintext
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-e1000-1/1)# isis bfd disable
```
isis reverse-metric

Configures the reverse metric value on a single IS-IS interface.

Syntax

isis reverse-metric [ value] [whole-lan] [te-def-metric]

no isis reverse-metric [ value] [whole-lan] [te-def-metric]

Command Default

The isis reverse-metric command is disabled by default.

Parameters

isis reverse-metric Specifies the reverse metric parameter at the interface level.
value Specifies the reverse metric value in metric style. The metric style consists of narrow or wide style. The narrow metric range is from 1 - 63. The wide metric range is from 1 - 16777215. The default value is 16777214 irrespective of the metric style configured. If the reverse-metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor router receives the reverse metric value through the IS hello, the neighbor router updates the cost to reach the original IS-IS router with the sum of default metric and the reverse metric value. This helps in shifting traffic to the other alternate paths.

whole-lan Specifies changing the reverse metric parameter for the entire LAN. The whole-lan option indicates the whole LAN bit in the flag. If the whole-lan option is enabled, the configured reverse metric value affects the entire LAN. If the whole-lan option is not enabled, the reverse metric value affects only the neighbor router. This option takes effect only on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the whole-lan option is enabled.

te-def-metric Specifies setting the TE default metric sub-TLV. If the te-def-metric option is enabled, the router sends a TE default metric sub-TLV within the reverse-metric TLV.

Modes

IS-IS interface level.

Usage Guidelines

Use the isis reverse-metric command when you are performing network maintenance operations, such as software upgrades, at the link level. When maintenance operations are performed, the link undergoing maintenance should not be used by the neighbor routers to forward transit traffic. In order to shift traffic away from the link undergoing maintenance, configure the isis reverse-metric command on the maintenance link. The router undergoing maintenance first advertises a reverse metric TLV in a IS-IS hello PDU to its neighbor router on a point-to-point or multi-access link. When the neighbor router receives a high reverse metric value, the router selects alternate paths to forward traffic while maintenance is going on. The neighbor router adds the reverse metric TLV to its own TE default metric sub-TLV and recalculates its SPF tree and route topology. The neighbor router floods the new LSP containing the extended IS reachability TLV throughout the domain. Traffic gradually shifts onto alternate paths away from the link between the maintenance router and the neighbor router as nodes in the IS-IS domain receive the new LSP. Once the maintenance is complete, you can remove the isis reverse-metric command configuration on the link, and the reverse metric TLV in the IS-IS hello PDU is no longer advertised to the neighbor router. The IS-IS neighbor router reverts back to its original IS-IS metric, and the traffic switches to the original IS-IS link to reach its destination.
In a multi-access link, the IS-IS DIS router adds the reverse metric TLV value to each node's default metric value in the pseudonode LSP when the whole-lan flag is set. All non-DIS nodes ignore the reverse metric TLV. If multiple neighbor routers advertise the reverse metric TLV with the whole LAN flag set, the neighbor router with the highest MAC address takes precedence, and the value advertised by that neighbor is updated in the pseudonode LSP for all neighbors. If some neighbor routers do not set the whole LAN flag, then the reverse metric TLV value advertised by the neighbor router is updated in the pseudonode LSP for that neighbor only.

The S flag is set when the sender of the reverse metric TLV signals to the neighbor router to use the TE sub-tlv for the default metric (sub-tlv type 18) in the reverse metric TLV. When the receiving router finds the S flag set in the reverse metric TLV, the router searches for the TE sub-tlv. The router adds the default metric value in the TE sub-tlv to the configured TE default metric value and recalculates the CSPF.

The no form of the command, specified with the configured value, resets the metric value to the default value of 16777214. The no isis reverse-metric command removes the entire reverse metric configuration.

**NOTE**

The isis reverse-metric value command is supported on the Brocade NetIron XMR Series, the Brocade MLX Series, and the Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

**Examples**

The following example configures the reverse metric value to 40 on a single IS-IS interface level. The whole-lan option is enabled to include the entire LAN.

```
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2)# isis reverse-metric ?
DECIMAL Narrow metric range 1-63, Wide metric range 1-16777214,
Default is 16777214
 te-def-metric Update TE default metric sub-tlv
 whole-lan Change metric for whole LAN
device(config-if-e1000-2/2)# isis reverse-metric 40 ?
te-def-metric Update TE default metric sub-tlv
 whole-lan Change metric for whole LAN
 <cr>
device(config-if-e1000-2/2)# isis reverse-metric 40 whole-lan
device(config-if-e1000-2/2)#
```
Use the `show isis` command to display the configuration of the reverse metric value at the global level. The reverse metric value and flags are highlighted in the output.

device(config)# show isis
IS-IS Routing Protocol Operation State: Enabled
IS-Type: Level-1-2
System ID: aaaa.bbbb.cccc
Manual area address(es):
  49.2211
Level-1-2 Database State: On
Administrative Distance: 115
Maximum Paths: 4

ISIS Global Reverse Metric 40
ISIS Global Reverse Metric Flags: W S

Use the `show isis interface` command to display the configuration of the reverse metric value at the interface level. The reverse metric value and flags are highlighted in the output.

device(config)# show isis interface
Total number of IS-IS Interfaces: 1

Interface: eth 1/1
  Circuit State: DOWN Circuit Mode: LEVEL-1-2
  Circuit Type: BCAST Passive State: FALSE
  Circuit Number: 1, MTU: 1500
  Level-1 Auth-mode: None
  Level-2 Auth-mode: None
  Level-1 Metric: 10, Level-1 Priority: 64
  Level-1 Hello Interval: 10 Level-1 Hello Multiplier: 3
  Level-1 Designated IS: MLX-2-01 Level-1 DIS Changes: 1
  Level-2 Metric: 10, Level-2 Priority: 64
  Level-2 Hello Interval: 10 Level-2 Hello Multiplier: 3
  Level-2 Designated IS: MLX-2-01 Level-2 DIS Changes: 1

  IP Enabled: TRUE
  IPv6 Enabled: FALSE
  MPLS TE Enabled: FALSE
  ISIS Reverse Metric 40
  ISIS Reverse Metric Flags: W S
  LDP-SYNC: Disabled, State: -

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**jitc enable**

Enables the Joint Interoperability Test Command (JITC) mode.

**Syntax**

```
  jitc enable
  no jitc enable
```

**Command Default**

JITC is not enabled.

**Modes**

Global configuration mode.

**Usage Guidelines**

When JITC is enabled, the Advanced Encryption Standard - Cipher-Block Chaining (AES-CBC) encryption mode for the Secure Shell (SSH) protocol is disabled and the AES-CTR (Counter) encryption mode is enabled. To enable the AES-only mode for SSH, use the `ip ssh encryption aes-only` command. To disable the AES-CBC encryption mode, use the `ip ssh encryption disable-aes-cbc` command. When the `jitc enable` command is configured, the `ip ssh encryption aes-only` command and the `ip ssh encryption disable-aes-cbc` command are automatically enabled.

When JITC is enabled, the MD5 authentication scheme for NTP is disabled. The SHA1 authentication scheme is available to define the authentication key for NTP.

The `no` form of the command disables the JITC mode and puts the system back to the standard mode and enables both AES-CBC encryption mode and MD5 authentication configuration. The `ip ssh encryption disable-aes-cbc` command is removed from the running configuration. The `ip ssh encryption aes-only` command configuration is retained in the running configuration.

**Examples**

The following example enables the JITC mode.

```
device# configure terminal
device(config)# jitc enable
```
In the output below, when the JITC mode is configured, the running configuration displays MD5 as disabled. The `ip ssh encryption aes-only` command and the `ip ssh encryption disable-aes-cbc` command are enabled. The commands are highlighted below.

**NOTE**

In the output below, the authentication-key entry is displayed when the authentication key for NTP is configured separately.

```
device(config)# show run | begin jitc
jitc enable
!
ntp
disable authenticate md5
authentication-key key-id 1 sha1 2 $b24tb25V
!
ip ssh encryption aes-only
ip ssh encryption disable-aes-cbc
end
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
key-add-remove-interval

Alters the timing of the authentication key add-remove interval.

**key-add-remove-interval interval**

**no key-add-remove-interval interval**

The interval is 300 seconds.

<table>
<thead>
<tr>
<th>interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the add-remove interval in seconds. Valid values range from 0 through 14400. The default is 300.</td>
</tr>
</tbody>
</table>

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

The no form of the command sets the add-remove interval to the default value of 300 seconds.

The following example sets the key add-remove interval to 240 seconds.

```plaintext
device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# key-add-remove-interval 240
```

The following example sets the key add-remove interval to 210 seconds in a nondefault VRF instance:

```plaintext
device# configure terminal
device(config)# ipv6 router ospf vrf red
device(config-ospf6-router-vrf-red)# key-add-remove-interval 240
```
key-rollover-interval

Alters the timing of the existing configuration changeover.

Syntax

    key-rollover-interval interval
    no key-rollover-interval interval

Command Default

The interval is 300 seconds.

Parameters

    interval

        Specifies the key-rollover-interval in seconds. Valid values range from 0 through 14400. The default is 300.

Modes

    OSPFv3 router configuration mode
    OSPFv3 router VRF configuration mode

Usage Guidelines

In order to have consistent security parameters, rekeying should be done on all nodes at the same time. Use the key-rollover-interval command to facilitate this. The key rollover timer waits for a specified period of time before switching to the new set of keys. Use this command to ensure that all the nodes switch to the new set of keys at the same time.

The no form of the command sets the rollover interval to the default value of 300 seconds.

Examples

The following example sets the key rollover interval to 420 seconds.

    device# configure terminal
    device(config)# ipv6 router ospf
    device(config-ospf6-router)# key-rollover-interval 420

The following example re-sets the key rollover interval to the default value.

    device# configure terminal
    device(config)# ipv6 router ospf
    device(config-ospf6-router)# no key-rollover-interval 420

The following example re-sets the key rollover interval to the default value in a nondefault VRF instance.

    device# configure terminal
    device(config)# ipv6 router ospf vrf red
    device(config-ospf6-router-vrf-red)# no key-rollover-interval 420
key-server-priority

Configures the MACsec key-server priority for the MACsec Key Agreement (MKA) group to select key server.

Syntax

```
key-server-priority value
no key-server-priority value
```

Command Default

Key-server priority is set to 16. This is not displayed in configuration details.

Parameters

```
value
```

Specifies key-server priority. The possible values range from 0 to 255, where 0 is highest priority and 255 is lowest priority. Default is 16.

Modes

```
dot1x-mka-cfg-group mode.
```

Usage Guidelines

During key-server election, the server with the highest priority (the server with the lowest key-server priority value) becomes the key-server.

The **no** form of the command removes the previous priority setting.

Examples

The following example explains how to set the key-server priority for MKA group group1 to 20.

```
deviceenable
deviceconfigure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# key-server-priority 20
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
l2 policy route-map

Enables Layer 2 PBR by applying a route map that is configured for Layer 2 PBR on an interface.

Syntax

l2 policy route-map route-map-name
no l2 policy route-map route-map-name

Command Default

Layer 2 PBR is not enabled by default.

Parameters

route-map-name
Specifies the name of the route map to be applied on the physical interface.

Modes

Interface configuration mode.

Usage Guidelines

Layer 2 PBR cannot be applied globally. Layer 2 PBR can be applied only at the physical interface level.

If both Layer 2 PBR and Layer 3 PBR are applied on the same interface (or Layer 3 PBR is applied globally), Layer 2 PBR only filters non-IP packets. If only Layer 2 PBR is applied, Layer 2 PBR filters both IP and non-IP packets.

Layer 2 PBR cannot be applied on a VE interface.

Layer 2 PBR cannot be applied on an interface where Layer 2 ACL or Layer 3 ACL is already applied.

Layer 2 PBR cannot be applied on an interface where ACL-based rate limiting is already applied.

The no form of the command removes the route map applied on the interface.

Examples

The following example enables Layer 2 PBR by applying a route map that is configured for Layer 2 PBR on an interface.

deviceenable
deviceconfigure terminal
device(config)# mac access-list abc
device(config-mac-acl-abc)# permit any any any etype 8000
device(config-mac-acl-abc)# exit

device(config)# route-map pbr permit 1
device(config-routemap pbr)# match l2acl abc
device(config-routemap pbr)# set next-hop-flood-vlan 100
device(config-routemap pbr)# exit

device(config) interface ethernet 1/1
device(config-if-e10000-1/1)# l2 policy route-map pbr
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00b</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
**label-range static**

Configures the minimum and maximum values for user-configurable static labels.

**Syntax**

```
label-range static { min-value num | max-value num }
no label-range static { min-value num | max-value num }
```

**Parameters**

- **min-value**
  - Denotes the lower end of the range for the static labels.
  - `num` The range designation and can be between 16 - 499999. The default value is 16.

- **max-value**
  - Denotes the top end of the range for the static labels.
  - `num` The range designation and can be between 16 - 499999. The default value is 2047.

**Modes**

MPLS router mode (config-mpls).

**Usage Guidelines**

Labels are automatically distributed using LDP, RSVP or BGP. If a LSR is connected to a device that supports MPLS forwarding but does not support LDP, static labels can be used to maintain forwarding.

LDP, RSVP or BGP can be used to dynamically distribute label bindings. After an LSR receives labels, it installs the bindings into the `Label Forwarding Information Base (LFIB)` for MPLS forwarding.

- Static labels to IPv4 prefix binding
- Static cross-connects of labels
- To configure static label binding, define a static label range
- Cannot configure static labels for IPv4 VPN prefixes
- Bindings remain in LFIB even if the next hop LSR is down

The `no` form of the command restores the default to 16 for the min-value and to 2047 for max-value.

**Examples**

The following example displays the `label-range static` command:

```
device(config-mpls)# label-range static min 16 max 2047
```
label-withdrawal-delay

Delays sending a label withdrawal message for a FEC to a neighbor in order to allow the IGP and LDP to converge.

Syntax

```
label-withdrawal-delay secs
no label-withdrawal-delay secs
```

Command Default

The default is 60.

Parameters

`secs`

Specifies the delay period in seconds for the label withdrawal delay timer. The range is 0 - 300.

Modes

MPLS LDP configuration mode.

Usage Guidelines

Setting the `secs` variable to zero (0) disables the feature for subsequent events.

Setting the `secs` variable to a value in the range 1 - 300, updates the configured value.

When using the `no` form of the command to restore the default behavior, the specified value for the `secs` variable must match the configured value at the time that the `no` form of the command executes.

Examples

The following example sets the label withdrawal delay timer to 30 seconds.

```
device(config-mpls-ldp)# label-withdrawal-delay 30
```

The following example restores the command default behavior when the delay period configuration is already 30 seconds.

```
device(config-mpls-ldp)# no label-withdrawal-delay 30
```

The following example disables the label withdrawal delay timer.

```
device(config-mpls-ldp)# label-withdrawal-delay 0
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
License add
Installs the license file to the device.

Syntax

    license add { license file.xml }

Parameters

    license file.xml
    Specifies the license file to be installed on the flash.

Modes

    Privilege EXEC level.

Usage Guidelines

    Use this command to install the license to the device after the file is copied to the MP flash directory. To copy the license file to the MP flash directory, use the copy tftp flash command. Once the file is copied to the directory, use the license add command to install the license to the device.

    The command is not enabled by default.

Examples

    The following example installs the 10x10-20PUPG license to upgrade the system from 10-port to 20-port.

    device# license add 20150831003730756eydFIJM1FFr.xml

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
license delete

Removes the license file from the license database.

Syntax

```
license delete index_number
```

Parameters

```
index_number
```

The index_number variable is a valid license index number. The license index number can be retrieved from the `show license` command output.

Modes

Privileged EXEC level.

Usage Guidelines

The licensed feature will continue to run as configured until the software is reloaded, at which time the feature will be disabled and removed from the system. Syslog and trap messages are generated when the license is deleted.

Examples

The following example shows the command will remove the license for index number 7.

```
device# license delete 7
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**link-protection**

Enables link protection for an FRR enabled LSP.

**Syntax**

```
link-protection
no link-protection
```

**Command Default**

The default configuration is always node protection.

**Modes**

FRR-LSP mode (config-mpls-lsp-frr).

**Usage Guidelines**

The `no` function of the command sets protection type back to default behavior, which is node protection.

**Examples**

The following example displays the configuration example for an adaptive LSP:

```
device#configure terminal
device(config)# router mpls
device(config-mpls)# lsp t1
device(config-mpls-lsp-t1)# to 44.44.44.44
device(config-mpls-lsp-t1)# frr
device(config-mpls-lsp-t1-frr)# link-protection
device(config-mpls-lsp-t1)# enable
```

The following example displays the configuration example for a non-adaptive LSP:

```
device#configure terminal
device(config)# router mpls
device(config-mpls)# lsp t1
device(config-mpls-lsp-t1)# to 44.44.44.44
device(config-mpls-lsp-t1)# adaptive
device(config-mpls-lsp-t1)# enable
device(config-mpls)# lsp t1
device(config-mpls-lsp-t1)# frr
device(config-mpls-lsp-t1-frr)# link-protection
device(config-mpls-lsp-t1)# commit
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
local-as

Specifies the BGP autonomous system number (ASN) where the device resides.

Syntax

local-as num
no local-as num

Parameters

num

The local ASN. The range is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

Use the no form of this command to remove the ASN from the device.

ASNs in the range from 64512 through 65535 are private numbers that are not advertised to the external community.

Examples

This example assigns a separate local AS number.

device# configure terminal
device(config)# router bgp
device(config-bgp)# local-as 777
load-balance mask ip
Masks specific values during ECMP and LAG index hash calculations.

Syntax
load-balance mask ip [ dst-ip [ slot number | all | pre-symmetriclb ] | src-ip [ slot number | all | pre-symmetriclb ] | dst-l4-port | [ slot number | all ] | src-l4-port [ slot number | all ] | protocol [ slot number | all ] ]
no load-balance mask ip [ dst-ip [ slot number | all | pre-symmetriclb ] | src-ip [ slot number | all | pre-symmetriclb ] | dst-l4-port | [ slot number | all ] | src-l4-port [ slot number | all ] | protocol [ slot number | all ] ]

Command Default
The functionality is disabled by default.

Parameters
dst-ip
Masks the destination IP address.

pre-symmetriclb
Masks the IP address before symmetric load balancing can occur.

slot number
Identifies the slot number for the specific source or destination IP address, TCP or UDP source or destination port, or IPv4 protocol.

all
Applies the command to all ports within the device.

src-ip
Masks the source IP address.

dst-l4-port
Masks the Layer 4 destination port.

src-l4-port
Masks the Layer 4 source port.

protocol
Masks the IPv4 protocol ID.

Modes
Global configuration mode

Usage Guidelines
The no form of the command disables the masking of specified values during ECMP and LAG index hash calculations.
Examples

The following example masks all the Layer 4 source ports within the device.

device(config)# load-balance mask ip src-l4-port all

The following example masks the source IP address before symmetric load balancing can occur for the IPv4 traffic entering slot 10 of the device.

device(config)# load-balance mask ip src-ip pre-symmetriclb 10

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the <strong>pre-symmetriclb</strong> option.</td>
</tr>
</tbody>
</table>
load-balance mask ipv6

Masks specific values during ECMP and LAG index hash calculations for IPv6.

Syntax

```
load-balance mask ipv6 [ dst-ip [ slot number | all | pre-symmetriclb ] | src-ip [ slot number | all | pre-symmetriclb ] | dst-l4-port [ [ slot number | all ] | src-l4-port [ slot number | all ] | next-hdr [ slot number | all ] ]

no load-balance mask ipv6 [ dst-ip [ slot number | all | pre-symmetriclb ] | src-ip [ slot number | all | pre-symmetriclb ] | dst-l4-port [ [ slot number | all ] | src-l4-port [ slot number | all ] | next-hdr [ slot number | all ] ]
```

Command Default

The functionality is disabled by default.

Parameters

dst-ip

Masks the destination IPv6 address.

pre-symmetriclb

Masks the IPv6 address before symmetric load balancing can occur.

slot number

Identifies the slot number for the specific source or destination IPv6 address, TCP or UDP source or destination port, or IPv6 protocol.

all

Applies the command to all ports within the device.

src-ip

Masks the source IPv6 address.

dst-l4-port

Masks the Layer 4 destination port.

src-l4-port

Masks the Layer 4 source port.

next-hdr

Masks the IPv6 next header.

Modes

Global configuration mode

Usage Guidelines

The no form of the command disables masking of specified values during ECMP and LAG index hash calculations for IPv6.
Examples

The following example masks all the source IPv6 ports within the device.

device(config)# load-balance mask ipv6 src-ip all

The following example masks the destination IPv6 address before symmetric load balancing can occur for the IPv6 traffic entering on slot 5 of the device.

device(config)# load-balance mask ipv6 dst-ip pre-symmetriclb 5

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the pre-symmetriclb option.</td>
</tr>
</tbody>
</table>
local-certificate

Specifies the URL for the local peer certificate of a specific trustpoint.

Syntax

```plaintext
local-certificate url URL name
no local-certificate url URL name
```

Parameters

- **url**
  - Specifies the URL name for the local peer certificate.

- **URL name**
  - The URL name for the local peer certificate.

Modes

PKI trustpoint configuration mode.

Usage Guidelines

The `no` form of the removes the local certificate URL name.

Examples

The following example specifies the local certificate URL name as provided here.

```plaintext
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# local-certificate url http://WIN-HJ98AK136A0.englab.brocade.com/pki_local_cert
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
location

Configures the location for the Public Key Infrastructure (PKI) entity.

Syntax

location string

Parameters

string

Specifies name of the location for PKI entity.

Modes

PKI entity configuration mode

Examples

The following example configures the location for PKI entity.

device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# location brocade_location

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
log (OSPFv2)

Controls the generation of OSPFv2 logs.

Syntax

```
log { adjacency [ dr-only ] | all | bad_packet [ checksum ] | database | memory | retransmit }
no log { adjacency [ dr-only ] | all | bad_packet [ checksum ] | database | memory | retransmit }
```

Command Default

Only OSPFv2 messages indicating possible system errors are logged. Refer to the Parameters section for specific defaults.

Parameters

- **adjacency**
  Specifies the logging of essential OSPFv2 neighbor state changes. This option is disabled by default.
  - **dr-only**
    Specifies the logging of essential OSPF neighbor state changes where the interface state is designated router (DR).

- **all**
  Specifies the logging of all syslog messages.

- **bad-packet**
  Specifies the logging of bad OSPFv2 packets. This option is enabled by default.
  - **checksum**
    Specifies all OSPFv2 packets that have checksum errors.

- **database**
  Specifies the logging of OSPFv2 LSA-related information. This option is disabled by default.

- **memory**
  Specifies the logging of OSPFv2 memory issues. This option is enabled by default.

- **retransmit**
  Specifies the logging of OSPFv2 retransmission activities. This option is disabled by default.

Modes

- OSPF router configuration mode
- OSPF router VRF configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv2. If this command is not enabled only OSPFv2 messages indicating possible system errors are logged.
For interfaces where the designated router state is not applicable, such as point-to-point and virtual links, OSPF neighbor state changes are always logged irrespective of the setting of the `dr-only` sub-option.

A limitation with the `dr-only` sub-option is that when a DR/BDR election is underway, OSPF neighbor state changes pertaining to non-DR/BDR routers are not logged. Logging resumes once a DR is elected on that network.

The `no` form of the command restores the default settings. Use the `no log all` command to return all OSPFv2 logging options to the default settings.

Examples

The following example enables the logging of all OSPFv2-related syslog events.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# log all
```

The following example enables the logging of OSPFv2 retransmission activities.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# log retransmit
```
logging enable
Enables system log messages and traps for the specified protocol or event.

Syntax
logging enable { bfd | cfm | config-changed | fan-speed-change | fan-state-change | ikev2 | ikev2-extended | ipsec | link-state-change | mac-mismatch-detection | mgmt-mod-redun-state-change | module-hotswap | mpls | mvrp-vlan | ntp | ospf | pki-extended | rstp | snmp-auth-failure | temp-error | user-login | vrrp-config-validate | vrrp-if-state-change }
no logging enable { bfd | cfm | config-changed | fan-speed-change | fan-state-change | ikev2 | ikev2-extended | ipsec | link-state-change | mac-mismatch-detection | mgmt-mod-redun-state-change | module-hotswap | mpls | mvrp-vlan | ntp | ospf | pki-extended | rstp | snmp-auth-failure | temp-error | user-login | vrrp-config-validate | vrrp-if-state-change }

Command Default
Log messages for specific protocols or events are enabled.

Parameters
bfd
Specifies the log messages and traps for BFD.
cfm
Specifies the log messages and traps for CFM.
config-changed
Specifies the log messages and traps for configuration data changed.
fan-speed-change
Specifies the log messages and traps for fan speed change events.
fan-state-change
Specifies the log messages and traps for fan state change events.
ikev2
Specifies the log messages and traps for IKEv2 events.
ikev2-extended
Specifies the extended log messages and traps for IKEv2 events.
ipsec
Specifies the log messages and traps for IPsec events.
link-state-change
Specifies the log messages and traps for link state change events.
mac-mismatch-detection
Enables or disables the Ethernet MAC address and ARP MAC address mismatch detection syslog message.
mgmt-mod-redun-state-change
Specifies the log messages and traps for management module redundant state change events.
module-hotswap
  Specifies the log messages and traps for module inserted or removed events.

mpls
  Specifies the log messages and traps for MPLS events.

mvrp-vlan
  Specifies the log messages and traps for MVRP VLAN events.

ntp
  Specifies the log messages and traps for NTP events.

ospf
  Specifies the log messages and traps for OSPF events.

pki-extended
  Specifies the extended log messages and traps for IKEv2 events.

rstp
  Specifies the log messages and traps for RSTP events.

snmp-auth-failure
  Specifies the log messages and traps for SNMP authentication failure events.

temp-error
  Specifies the log messages and traps for temperature error events.

user-login
  Specifies the log messages and traps for login usernames.

vrrp-config-validate
  Specifies the log messages and traps for VRRP for configuration validation events.

vrrp-if-state-change
  Specifies the log messages and traps for VRRP if state change events.

Modes
  Global configuration mode.

Usage Guidelines
  The no form of the command disables the generation of the specified syslog messages and traps.

Examples
  The following example configures syslog generation for IPsec events.
  
  device(config)# logging enable ipsec

  The following example enables the syslog message to be displayed if there is any source MAC address mismatch between the Layer 2 Ethernet header and the ARP header.
  
  device(config)# logging enable mac-mismatch-detection
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to add the <code>mac-mismatch-detection</code> and <code>vrrp-config-validate</code> keywords to the syntax.</td>
</tr>
<tr>
<td>5.9.00a</td>
<td>This command was modified to add the <code>ikev2-extended</code> and <code>pki-extended</code> keywords to the syntax.</td>
</tr>
</tbody>
</table>
log-dampening-debug
Logs dampening debug messages.

Syntax
log-dampening-debug
no log-dampening-debug

Command Default
This option is disabled.

Modes
BGP configuration mode

Usage Guidelines
Use the no form of this command to restore the default.

Examples
The following example logs dampening debug messages.

device# configure terminal
device(config)# router bgp
device(config-bgp)# log-dampening-debug
log-status-change

Controls the generation of all OSPFv3 logs.

Syntax

    log-status-change
    no log-status-change

Command Default

Disabled

Modes

OSPFv3 router configuration mode
OSPFv3 router VRF configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of events related to OSPFv3, such as neighbor state changes and database overflow conditions.

The no form of this command disables the logging of events.

Examples

The following example disables the logging of events.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# no log-status-change

The following example enables the logging of events.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# log-status-change
**logs-per-interval-per-mep-rmep**

Limits the log generation of individual MEPs or RMEPs in a 15 minute time window.

**Syntax**

\[
\text{logs-per-interval-per-mep-rmep value} \\
\text{no logs-per-interval-per-mep-rmep value}
\]

**Command Default**

Limiting the log generation for MEPs or RMEPs is not enabled by default.

**Parameters**

\[value\]

Specifies the number of logs generated per MEP or RMEP per 900000 milliseconds. The decimal range is from 1 to 100. The default is 10.

**Modes**

CFM Protocol Configuration mode.

**Usage Guidelines**

Use the **logs-per-interval-per-mep-rmep** value command to limit the number of logs generated for each MEP or RMEP in a 15 minute time window. When the value parameter is configured, the value is uniform for all MEPs and RMEPs. The **no logs-per-interval-per-mep-rmep** value command resets the value to the default value.

**NOTE**


**Examples**

The following example limits the log generation to 20 logs per MEP or RMEP in a 15 minute time window.

```
device(config)#cfm-enable
device(config-cfm)#logs-per-interval-per-mep-rmep 20
device(config-cfm)#
```

Use the **show cfm logs-limit-per-mep-rmep** command to display the value parameter configured for the log limit generation for each MEP or RMEP. The value parameter is highlighted in the output.

```
device(config-cfm)# show cfm logs-limit-per-mep-rmep
Logs limit per interval (900000 ms) per MEP/RMEP : 20 (Default : 10)
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**lsr-id**

Enables the feature and sets the desired configured IP address for the feature.

**Syntax**

`lsr-id ip_addr`

**Parameters**

`ip_addr`  
The value set to use as the LSR-ID for LDP protocol.

**Modes**

MPLS configuration mode (config-mpls-ldp).

**Usage Guidelines**

When the **no** form of the command is executed and LDP protocol is in enabled state, it continues with same LSR-ID because the IP address selected as LSR-ID for LDP protocol is still valid and is the operationally UP IP address on an enabled loopback interface. When, at the time of disabling the feature, LDP protocol is in disabled state (this happens when the loopback interface on which IP address is configured is in the disabled state), the system falls back to default behavior which tries to enable LDP protocol when it finds a valid IP address on any one of the enabled loopback interfaces.

In order to disable the feature, specify the exact IP address during configuration of the feature.

The user can configure only the IPv4 address.

**Examples**

The following example displays the output of the `lsr-id` command:

```
device> enable
device# config t
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# lsr-id 22.22.22.22
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
mac access-group

Applies rules specified in a named or numbered MAC access control list (ACL) to traffic entering or exiting an interface.

Syntax

```
mac access-group { acl-num | acl-name } { in | out }
no mac access-group { acl-num | acl-name } { in | out }
```

Command Default

ACLs are not applied to interfaces.

Parameters

- **acl-num**
  Specifies an ACL number from 400 through 1399.

- **acl-name**
  Specifies an ACL name of up to 255 alphanumeric characters. The first character must be alphabetic.

- **in**
  Applies the ACL to inbound traffic on the port.

- **out**
  Applies the ACL to outbound traffic on the port.

Modes

Interface subtype configuration modes

Usage Guidelines

To apply a MAC ACL name that contains spaces, enclose the name in quotation marks (for example, `mac access-group "Deny-all ACL" in`).

To remove an ACL from an interface, use the **no** form of this command.

Examples

The following example creates a named MAC ACL, defines rules within, and then applies it to an interface.

```
device(config)# mac access-list example_l2_acl
device(config-mac-nacl)# deny 0000.0000.0001 ffff.ffff.ffff any
device(config-mac-nacl)# permit any 0000.0000.0002 ffff.ffff.ffff
device(config-mac-nacl)# exit
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2) #mac access-group example_l2_acl in
```
The first phase of the following example creates a numbered MAC ACL, containing rules that deny all ARP, IPv6, and MPLS multicast traffic; and permit all other traffic in VLAN 100.

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

The second phase of the example applies the ACL to a physical interface, to filter outbound traffic:

```
device(config)# interface ethernet 4/12
device(config-int-e100-4/12)# mac access-group 400 out
```
mac access-group enable-deny-logging

Running this command on an interface is one of the conditions for enabling logging of traffic denied by MAC ACLs applied to the interface. The other condition is the inclusion of the log parameter in rules within such ACLs.

Syntax

mac access-group enable-deny-logging [ hw-drop ]
no mac access-group enable-deny-logging [ hw-drop ]

Command Default

Deny-logging for MAC ACLs is disabled.

Parameters

hw-drop

Specifies that MAC ACL-log packets be dropped in hardware, which reduces CPU load.

Modes

Interface subtype configuration modes

Usage Guidelines

Deny-logging is supported for inbound ACLs only.

When this command is implemented with the hw-drop option, packet-counts of denied traffic will include only the first packet in each time cycle.

To disable MAC ACL deny-logging on an interface, use the no mac access-group enable-deny-logging command. You do not have to remove log parameters from ACLs and re-apply the ACLs.

To disable the hw-drop option, use the no mac access-group enable-deny-logging hw-drop command.

Examples

The following example implements MAC ACL deny-logging on an interface—for applied ACLs that contain rules with log parameters.

device# configure terminal
device(config)# interface ethernet 5/1
device(config-if-e1000-5/1)# mac access-group enable-deny-logging
mac access-list

Creates a named MAC access list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

```
mac access-list acl-name
no mac access-list acl-name
```

Command Default

No named MAC ACLs are defined.

Parameters

`acl-name`

Specifies a unique MAC ACL name. The name can be up to 255 characters, and must begin with an alphabetic character. If the name contains spaces, put it within quotation marks. Otherwise, no special characters are allowed, except for underscores and hyphens.

Modes

Global configuration mode

Usage Guidelines

After you create a named ACL, enter one or more \[ sequence \] \{ permit | deny \} commands to create filtering rules for that ACL.

You can create up to 500 named MAC ACLs.

A MAC ACL starts functioning only after it is applied to an interface using the `mac access-group` command.

You can create numbered MAC ACLs, using the `access-list` command.

The system supports the following MAC ACL resources:

- Numbered MAC ACLs—1000
- Named MAC ACLs—500
- Maximum filter-rules per MAC ACL—64. You can change the maximum up to 256 by using the `system-max l2- acl-table-entries` command.

The `no` form of this command deletes the ACL. You can delete a MAC ACL only after you first remove it from all interfaces to which it is applied, using the `no mac access-group` command.
Examples

The following example creates a named MAC ACL, defines rules within, and then applies it to an interface.

device(config)#mac access-list example_l2_acl
device(config-mac-nacl)#deny 0000.0000.0001 ffff.ffff.ffff any
device(config-mac-nacl)#permit any 0000.0000.0002 ffff.ffff.ffff
device(config-mac-nacl)#exit
device(config)# interface ethernet 2/2
device(config-if-e1000-2/2)#mac access-group example_l2_acl in
mac-age-time

Tunes the system so it can function the most effectively based on the deployment and a specific configuration.

Syntax

mac-age-time [ dec | vpls { local | remote } ]

Parameters

dec

Sets the aging period, in seconds, to age the software MAC table.

vpls

Sets the aging period for VPLS mac entries.

local

MAC entries learned from local endpoints.

remote

MAC entries learned from PW.

Modes

Global configuration mode.

Usage Guidelines

- The values are bound by the same global system range shared with the regular MAC entries.
- The default values remain the same, which are 300 seconds for VPLS local entries and 600 seconds for the remote entries.
- Age time ‘0’ disables the software aging. VPLS MAC follows the same format to be consistent. However, the value ‘0’ is hidden as the valid range.
- When the software aging is disabled after the hardware aging is kicked in, and the software aging has already started, the age field displays the time value that elapsed prior to the aging being disabled.
- When the aging is re-enabled after a disable, the software aging resumes from the age value where it was stopped.
- Under the node vpls, you can specify a separate timer value for the local and the remote timers.
- The VPLS age timers are fully configurable for both local and remote entries.
- The formula ‘2 x’ between the local timer and the remote timer is removed. Now, you have the flexibility to specify values for the age timers independently for the local and the remote entries.

Examples

The following example displays a sample configuration for the mac-age-time command:

device(config)# mac-age-time vpls remote 240
## History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
**mac-move-det-syslog**

Enables the display of MAC movement syslog messages.

**Syntax**

- `mac-move-det-syslog`
- `no mac-move-det-syslog`

**Command Default**

By default, MAC movement syslog messages are displayed.

**Modes**

- Global configuration mode

**Usage Guidelines**

The **no** form of the command disables the display of MAC movement syslog messages.

**NOTE**

This command is only supported on Brocade NetIron MLX Series devices.
Examples

The following example shows the MAC movement syslog message output when `mac-move-det-syslog` command is used.

```plaintext
device(config)# mac-move-det-syslog
device(config)# show arp

Total number of ARP entries: 2
(In all VRFs)

Entries in default routing instance:
IP Address  MAC Address     Type     Age Port (Vpls-Id, Vlan)/ Vpls-Id:Peer
1  10.19.19.1    0010.9400.0606  Dynamic  1   1/24
2  172.26.67.1   0024.381c.b900  Dynamic  1   mgmt1
device(config)# exit
device#

SYSLOG: <12>Sep 25 02:43:07 IP/ARP: IP address 19.19.19.1 MAC movement detected,
changed from MAC 0010.9400.0606 / port 1/24 to MAC 0010.9400.0001 / port 1/24

device#
device# configure terminal
device(config)# show arp

Total number of ARP entries: 2
(In all VRFs)

Entries in default routing instance:
IP Address  MAC Address     Type     Age Port (Vpls-Id, Vlan)/ Vpls-Id:Peer
1  10.19.19.1    0010.9400.0001  Dynamic  1   1/24
2  172.26.67.1   0024.381c.b900  Dynamic  2   mgmt1
device(config)#
device(config)#

SYSLOG: <12>Sep 25 02:43:40 IP/ARP: IP address 19.19.19.1 MAC movement detected,
changed from MAC 0010.9400.0001 / port 1/24 to MAC 0010.9400.0606 / port 1/24

The following example shows the MAC movement syslog message output when the display is disabled.

device(config)# no mac-move-det-syslog
device(config)# exit
device# show arp

Total number of ARP entries: 2
(In all VRFs)

Entries in default routing instance:
IP Address  MAC Address     Type     Age Port (Vpls-Id, Vlan)/ Vpls-Id:Peer
1  10.19.19.1    0010.9400.0001  Dynamic  1   1/24
2  172.26.67.1   0024.381c.b900  Dynamic  2   mgmt1
device(config)#

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**macsec cipher-suite**

Enables GCM-AES-128 bit encryption or GCM-AES-128 bit integrity checks on MACsec frames transmitted between group members.

**Syntax**

```plaintext
macsec cipher-suite gcm-aes-128 [ integrity-only ]
no macsec cipher-suite gcm-aes-128 [ integrity-only ]
```

**Command Default**

By default GCM-AES-128 bit encryption or integrity checking is not enabled. Frames are encrypted starting with the first byte of the data packet, and ICV checking is enabled.

**Parameters**

- `gcm-aes-128`
  
  Enables GCM-AES-128 bit encryption.

- `integrity-only`
  
  Enables GCM-AES-128 bit integrity checks.

**Modes**

`dot1x-mka-cfg-group` mode.

**Usage Guidelines**

The `macsec cipher-suite` command can be used in conjunction with an encryption offset configured using the `macsec confidentiality-offset` command.

The no form of the command restores the default encryption and integrity checking.

**NOTE**

- When cipher suite is configured without integrity the capability of the system is confidentiality and integrity plus confidentiality offset 0.
- When integrity only is configured, then confidentiality offset configuration is not allowed and vice-versa.

**Examples**

The following example enables GCM-AES-128 encryption for group1.

```plaintext
device# configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec cipher-suite gcm-aes-128
```
The following example enables GCM-AES-128 bit integrity checking for group1.

device# configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec cipher-suite gcm-aes-128 integrity-only

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
macsec confidentiality-offset

Configures the offset size for MACsec encryption.

Syntax

```
macsec confidentiality-offset size
no macsec confidentiality-offset size
```

Command Default

By default the offset size is set to 0.

Parameters

```
size
```

Specifies the off-set value of 0 bytes. Valid values are:

```
0
  Complete packet is encrypted.
30
  Encryption begins at byte 31 of the data packet.
50
  Encryption begins at byte 51 of the data packet.
```

Modes

```
dot1x-mka-cfg-group mode
```

Usage Guidelines

The no form of the command disables encryption offset on all interfaces in the MACsec MKA group.

This command is applicable only when encryption is enabled for the MACsec group using the `macsec cipher-suite` command.

**NOTE**

Configuring the confidentiality off-set value to 0 bytes is not allowed.

Examples

The following example configures a 30-byte offset on encrypted transmissions as part of the parameters for group1.

```
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec confidentiality-offset 30
```
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
macsec frame-validation

Enables validation checks for frames with MACsec headers and configures the validation mode (strict or not strict).

Syntax

`macsec frame-validation [ disable | check | strict ]`
`no macsec frame-validation [ disable | check | strict ]`

Command Default

By default strict parameter is set as frame-validation mode.

Parameters

- `disable`
  Disables validation checks for frames with MACsec headers.

- `check`
  Enables validation checks for frames with MACsec headers and configures non-strict validation mode. If frame validation fails, counters are incremented but packets are accepted.

- `strict`
  Enables validation checks for frames with MACsec headers and configures strict validation mode. If frame validation fails, counters are incremented and packets are dropped.

Modes

`dot1x-mka-cfg-group mode`.

Usage Guidelines

The no form of the command restores the default mode of validation, (validation checks for frames with MACsec headers is disabled).

Examples

The following example enables validation checks for frames with MACsec headers on group group1 and configures strict validation mode.

```
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec frame-validation check
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
macsec replay-protection

Specifies the action to be taken when packets are received out of order, based on their packet number. If replay protection is configured, you can specify the window size within which out-of-order packets are allowed.

Syntax

macsec replay-protection [ strict | out-of-order window-size size ]
no macsec replay-protection [ strict | out-of-order window-size size ]

Command Default

Macsec replay protection is enabled in Strict mode.

Parameters

strict

Does not allow out-of-order packets.

out-of-order window size size

Specifies the allowable window within which an out-of-order packet can be received. Allowable range is from 1 through 4294967295.

Modes

dot1x-mka-cfg-group mode

Usage Guidelines

The no form of the command disables macsec replay protection.

Examples

The following example configures group group1 to accept packets with window size 100.

device# configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)# macsec replay-protection out-of-order window-size 100

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
match additional paths advertise-set

Matches the additional BGP paths that are candidates to be advertised in a route map instance.

Syntax

match additional paths advertise-set { all | best number | best-range start-range end-range | group-best }
no match additional paths advertise-set { all | best number | best-range start-range end-range | group-best }

Command Default

Paths are not matched.

Parameters

all

Specifies all paths.

best

Specifies the paths that the device selects as best paths.

number

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

best-range start-range end-range

Specifies a range of best paths. Valid values range from 1 through 16.

group-best

Specifies the group best paths.

Modes

Route map configuration mode

Usage Guidelines

This command can only be configured once in any route map instance. Once it is used in a route map instance, any subsequent use overwrites the existing configuration.

The no form of the command removes the BGP additional paths match statement from the route map instance.

Examples

The following example matches the nine best BGP paths as additional BGP paths that are candidates to be advertised.

device# configure terminal
device(config)# route-map myroutemap permit 1
device(config-route-map myroutemap)# match additional paths advertise-set 9
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
match identity
Configures the selection of IKEv2 profile Peer Authorization Database (PAD) for a peer based on local or remote identity parameters received.

Syntax

match identity {local {address ip address | dn dn name | email email address | fqdn fqdn name | key-id key ID name } | remote {address ip address | dn dn name | email email address | fqdn fqdn name | key-id key ID name } }

no match identity {local {address ip address | dn dn name | email email address | fqdn fqdn name | key-id key ID name } | remote {address ip address | dn dn name | email email address | fqdn fqdn name | key-id key ID name } }

Parameters

ipv4 address
Specifies the local IP address in the identity parameter received.

dn name
Specifies the DN value.

email address
Specifies the email address.

fqdn name
Specifies the FQDN name.

key id name
Specifies the key ID name.

ipv4 address
Specifies the remote IP address in the identity parameter received.

dn name
Specifies the DN name for the remote identity parameter received.

email address
Specifies the email address for the remote identity parameter received.

fqdn name
Specifies the FQDN name for the remote identity parameter received.

key id name
Specifies the key ID name for the remote identity parameter received.

Modes

IKEv2 profile configuration mode

Usage Guidelines

no
Examples

The following example configures the selection of IKEv2 profile (PAD) for a peer based on local IPv4 address.

device(config)# ikev2 profile brocade
device(config-ikev2-profile-brocade)# match identity local address 10.20.20.10

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**match l2acl**

Configures a route map that matches with the configured Layer 2 ACL.

**Syntax**

```
match l2acl { acl-number | acl-name }
no match l2acl { acl-number | acl-name }
```

**Command Default**

The Layer 2 ACL information is not configured in the route map configuration.

**Parameters**

- `acl-number`
  
  Specifies the numbered Layer 2 ACL.

- `acl-name`
  
  Specifies the named Layer 2 ACL.

**Modes**

Route map configuration mode.

**Usage Guidelines**

Five Layer 2 ACLs separated by spaces can be added in the `match l2acl` configuration of the route map.

The `no` form of the command removes the Layer 2 ACL match statement from the route map.

**Examples**

The following example configures a route map that matches with the configured Layer 2 ACL.

```
device(config)# route-map xGW_map permit 1
device(config-route-map xGW_map)# match l2acl abc
```

The following example configures multiple Layer 2 ACLs to a route map.

```
device(config)# route-map xGW_map permit 1
device(config-route-map xGW_map)# match l2acl 400 401 402
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00b</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
**med-missing-as-worst**

Configures the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

**Syntax**

```
med-missing-as-worst
no med-missing-as-worst
```

**Command Default**

This option is disabled.

**Modes**

BGP configuration mode

**Usage Guidelines**

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

When MEDs are compared, by default the device favors a low MED over a higher one. Because the device assigns a value of 0 to a route path MED if the MED value is missing, the default MED comparison results in the device favoring the route paths that do not have MEDs.

**Examples**

This example configures the device to favor a route containing a MED.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# med-missing-as-worst
```
method

Configures the IKEv2 authentication method.

Syntax

```
method {local {ecdsa384 | pre-shared} | remote {ecdsa384 | pre-shared} }
no method {local {ecdsa384 | pre-shared} | remote {ecdsa384 | pre-shared} }
```

Parameters

- **local**
  - Specifies the local authentication method.
- **remote**
  - Specifies the remote authentication method.
- **ecdsa384**
  - Specifies the digital signature for the authentication certificate.
- **pre-shared**
  - Specifies the pre-shared key value.

Modes

IKEv2 auth-proposal configuration mode

Usage Guidelines

no

Examples

The following example configures IKEv2 authentication method.

```
device(config)# ikev2 auth-proposal brocade
device(config-ike-auth-brocade)# method local ecdsa384
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**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-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 255.

Modes

VLAN configuration mode

Usage Guidelines

If you plan to use a topology group to add VLANs to the ring, make sure you configure MRP on the topology group master VLAN.

If you want to add more than one metro ring to a port-based VLAN, use the `metro-rings` command.

The `no` form of the command removes the metro ring from the port-based VLAN.

Examples

The following example shows how to add the metro ring to a port-based VLAN.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)#
```
**mka-auth-fail-action**

Configures MACsec Key Agreement (MKA) authentication fail action on MKA group.

**Syntax**

```
mka-auth-fail-action [ allow-unencrypted-traffic | deny-all-traffic ]
no mka-auth-fail-action [ allow-unencrypted-traffic | deny-all-traffic ]
```

**Command Default**

By default, `deny-all-traffic` is enabled.

**Parameters**

- **allow-unencrypted-traffic**
  
  Allows unencrypted traffic exchange between peers, even if MKA authentication fails.

- **deny-all-traffic**
  
  Drops all traffic exchange between peers, if MKA authentication fails.

**Modes**

MKA group configuration mode.

**Usage Guidelines**

The key-server is elected by comparing key-server priority values during MKA message exchange between peer devices. In case no peer is elected as key server then the MKA protocol moves to failed state. Under such scenario default behavior is to drop all the traffic on the link. However this behavior can be controlled using `mka-auth-fail-action` command by allowing unencrypted traffic exchange between peer devices even if MKA protocol fails.

The `no` form of the command disables MKA authentication fail action configuration on MKA group.

**Examples**

The following example explains how to configure MKA authentication fail action on MKA group.

```
device(config)#dot1x-mka-enable
device(config-dot1x-mka)#mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)#mka-auth-fail-action allow-unencrypted-traffic
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
mka-cfg-group

Configures a MACsec Key Agreement (MKA) configuration groups and enabling this command will enter into mka-cfg-group mode.

Syntax

mka-cfg-group group-name

no mka-cfg-group group-name

Parameters

group-name

Specifies the MKA configuration group name that can be applied to ports.

Modes

dot1x-mka configuration mode.

Usage Guidelines

The dot1x-mka-enable command must be executed before the mka-cfg-group command can be used.

NOTE

1. When a group is created, all group parameters will be assigned with the default values.
2. Maximum number of groups allowed is 128.

The no form of this command deletes the MKA configuration group.

Examples

The following example configures the MKA configuration group, group1.

device(config-dot1x-mka)# mka-cfg-group group1
device(config-dot1x-mka-cfg-group-group1)#

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
neighbor bfd

Enables Bidirectional Forwarding Detection (BFD) sessions for specified BGP neighbors or peer groups.

Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } bfd { holdover-interval time | min-tx transmit-time min-rx receive-time multiplier number }
```

```
no neighbor { ip-address | ipv6-address | peer-group-name } bfd { holdover-interval time | min-tx transmit-time min-rx receive-time multiplier number }
```

Command Default

BFD sessions are not enabled on specific BGP neighbors or peer groups.

Parameters

- **ip-address**
  Specifies the IP address of the neighbor.

- **ipv6-address**
  Specifies the IPv6 address of the neighbor.

- **peer-group-name**
  Specifies a peer group.

- **holdover-interval time**
  Specifies the holdover interval, in seconds, for which BFD session down notifications are delayed before notification that a BFD session is down. Valid values range from 1 through 30.

- **min-tx transmit-time**
  Specifies the interval, in milliseconds, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000. The default value is 1000 (unless changed at the global level).

- **min-rx receive-time**
  Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000. The default value is 1000 (unless changed at the global level).

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

Modes

- BGP configuration mode
- BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

Before using the `holdover-interval`, `min-tx`, `min-rx`, and `multiplier` parameters, you must first enable BFD.
When Brocade NetIron CER Series or Brocade NetIron CES Series devices are heavily loaded or under stress, BFD sessions may flap if the configured BFD interval is less than 500 milliseconds with a multiplier value of 3.

The no form of this command removes the BFD for BGP configuration for BGP neighbors or peer groups.

**Examples**

The following example sets the BFD holdover interval for a specified peer group to 18.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor pgl bfd holdover-interval 18
```

The following example sets the BFD session timer values for a BGP neighbor with the IP address 10.1.1.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor 10.1.1.1 bfd min-tx 120 min-rx 150 multiplier 8
```

The following example sets the BFD session timer values for a BGP neighbor with the IP address 10.1.1.1 for VRF "red" in BGP address-family IPv4 unicast VRF configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 10.1.1.1 bfd min-tx 120 min-rx 150 multiplier 8
```
neighbor additional-paths

Enables additional paths capability for specified BGP neighbors.

Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } additional-paths receive [ send ]
neighbor { ip-address | ipv6-address | peer-group-name } additional-paths send [ receive ]
no neighbor { ip-address | ipv6-address | peer-group-name } additional-paths receive [ send ]
no neighbor { ip-address | ipv6-address | peer-group-name } additional-paths send [ receive ]
```

Command Default

Additional paths are not advertised.

Parameters

- `ip-address`
  IPv4 address of the neighbor.

- `ipv6-address`
  IPv6 address of the neighbor.

- `peer-group-name`
  Peer group name configured by the `neighbor peer-group-name` command.

- `receive`
  Enables BGP capability to receive additional paths from BGP neighbors.

- `send`
  Enables BGP capability to send additional paths to BGP neighbors.

Modes

- BGP address-family IPv4 unicast configuration mode
- BGP address-family IPv6 unicast configuration mode
- BGP address-family IPv4 multicast configuration mode
- BGP address-family IPv6 multicast configuration mode
- BGP address-family IPv4 unicast VRF configuration mode
- BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Capability configured at the peer level using this command overrides any send or receive capability configured at the address-family or peer-group level using the `additional-paths` command.
Examples

The following example enables BGP4 capability to send additional paths to a specified BGP neighbor.

device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.11.12.13 additional-paths send

The following example enables BGP4+ capability to receive additional paths from a specified BGP neighbor.

device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 additional-paths receive

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
neighbor additional-paths advertise

Applies filters for the advertisement of additional paths for BGP neighbors.

Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } additional-paths advertise all [ best number ] [ group-best ]
neighbor { ip-address | ipv6-address | peer-group-name } additional-paths advertise best number [ all ] [ group-best ]
neighbor { ip-address | ipv6-address | peer-group-name } additional-paths advertise group-best [ all ] [ best number ]
no neighbor { ip-address | ipv6-address | peer-group-name } additional-paths advertise { all | best number | group-best }
```

Command Default

Filters are not applied.

Parameters

- **ip-address**
  IPv4 address of the neighbor.
- **ipv6-address**
  IPv6 address of the neighbor.
- **peer-group-name**
  Peer group name configured by the `neighbor peer-group-name` command.
- **all**
  Advertises all BGP additional paths with a unique next hop. The maximum number of paths is 16.
- **best**
  Advertises the additional paths that the device selects as best paths.
- **number**
  Specifies the number of best paths advertised. Valid values range from 2 through 16.
- **group-best**
  Specifies the group best paths. If the rank of any group-best add-path is more than 16, its is not advertised.

Modes

- BGP address-family IPv4 unicast configuration mode
- BGP address-family IPv6 unicast configuration mode
- BGP address-family IPv4 multicast configuration mode
- BGP address-family IPv6 multicast configuration mode
- BGP address-family IPv4 unicast VRF configuration mode
- BGP address-family IPv6 unicast VRF configuration mode
Usage Guidelines

The set of paths to be advertised must be a subset of the selected paths configured using the `additional-paths select` command.

The `no` form of the command disables the configured filter.

Examples

The following example configures BGP4 to advertise all BGP additional paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.11.12.13 additional-paths advertise all
```

The following example configures BGP4+ to advertise the four best BGP additional paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 additional-paths advertise best 4
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
neighbor additional-paths disable

Disables the advertisement of additional paths for specified BGP neighbors or peer groups.

Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } disable
no neighbor { ip-address | ipv6-address | peer-group-name } disable
```

Command Default

Disabled.

Parameters

- **ip-address**
  - IPv4 address of the neighbor.
- **ipv6-address**
  - IPv6 address of the neighbor.
- **peer-group-name**
  - Peer group name configured by the `neighbor peer-group-name` command.

Modes

- BGP address-family IPv4 unicast configuration mode
- BGP address-family IPv6 unicast configuration mode
- BGP address-family IPv4 multicast configuration mode
- BGP address-family IPv6 multicast configuration mode
- BGP address-family IPv4 unicast VRF configuration mode
- BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

If the capability to send and receive additional paths is configured at the address family level using the `additional-paths` command, this capability is applied to all the neighbors under the address family. Use this command to disable this capability for a specified neighbor or peer group.

When additional-path capability is enabled at the peer-group or address-family level, this command can be used to disable the capability at the neighbor level. When additional-path capability is enabled at the address family level, this command can be used to disable the capability at the peer-group level.
Examples

The following example disables the sending of additional paths by BGP4 to a specified BGP neighbor.

```bash
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.11.12.13 additional-paths disable
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
neighbor ebgp-btsh

Enables BGP time to live (TTL) security hack protection (BTSH) for eBGP.

Syntax

`neighbor { ip-address | ipv6-address | peer-group-name } ebgp-btsh`

`no neighbor { ip-address | ipv6-address | peer-group-name } ebgp-btsh`

Command Default

Disabled.

Parameters

- `ip-address`
  - Specifies the IPv4 address of the neighbor.

- `ipv6-address`
  - Specifies the IPv6 address of the neighbor.

- `peer-group-name`
  - Specifies a peer group.

Modes

- BGP configuration mode
- BGP address-family IPv6 unicast configuration mode
- BGP address-family IPv6 multicast configuration mode
- BGP address-family IPv4 unicast VRF configuration mode
- BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

When this command is entered in BGP global configuration mode, it applies only to the IPv4 address family. Use this command in BGP address-family IPv6 unicast configuration mode for BGP4+ configurations. To maximize the effectiveness of this feature, the `neighbor ebgp-btsh` command should be executed on each participating device.

The `neighbor ebgp-btsh` command is supported for both directly connected peering sessions and multihop eBGP peering sessions. When the `neighbor ebgp-btsh` command is used, BGP control packets sent by the device to a neighbor have a TTL value of 255. In addition, the device expects the BGP control packets received from the neighbor to have a TTL value of either 254 or 255. For multihop peers, the device expects the TTL for BGP control packets received from the neighbor to be greater than or equal to 255, minus the configured number of hops to the neighbor. If the BGP control packets received from the neighbor do not have the anticipated value, the device drops them.

The `no` form of the command disables BTSH for eBGP.
Examples

The following example enables GTSM between a device and a neighbor with the IP address 10.10.10.1.

device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor 10.1.1.1 ebgp-btsh

The following example enables GTSM between a device and a neighbor with the IPv6 address 2001:2018:8192::125.

device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 prefix-list ebgp-btsh
neighbor fail-over

Enables or disables Bidirectional Forwarding Detection (BFD) protocol support for failover.

Syntax

neighbor { ip-address | ipv6-address | peer-group-name } fail-over { bfd-enable | bfd-disable }

no neighbor { ip-address | ipv6-address | peer-group-name } fail-over { bfd-enable | bfd-disable }

Command Default

BFD support for failover is disabled.

Parameters

ip-address

Specifies the IP address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

bfd-enable

Enables BFD support for failover.

bfd-disable

Disables BFD support for failover.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

The no form of the command disables BFD support for failover.

Examples

The following example enables BFD support for failover for a BGP neighbor with the IP address 10.1.1.1.

device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor 10.1.1.1 fail-over bfd-enable
The following example enables BFD support for failover for a BGP neighbor with the IP address 10.1.1.1 for VRF instance “blue” in BGP address-family IPv4 unicast VRF configuration mode.

device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast vrf blue
device(config-bgp-ipv4u-vrf)# neighbor 10.1.1.1 fail-over bfd-enable

The following example enables BFD support for failover for a BGP peer group.

device# configure terminal
device(config)# router bgp
device(config-bgp-ipv4u-vrf)# neighbor pg1 fail-over bfd-enable
neighbor next-hop-self (BGP)

Causes the device to list itself as the next hop in updates that are sent to the specified neighbor.

Syntax

```
neighbor ip-address | ipv6-address | peer-group-name next-hop-self [ always ]
no neighbor ip-address | ipv6-address | peer-group-name next-hop-self
```

Parameters

- **ip-address**: The IPv4 address of the neighbor.
- **ipv6-address**: The IPv6 address of the neighbor.
- **peer-group-name**: The peer group name configured by the `neighbor peer-group-name` command.
- **always**: Enables this feature for route reflector (RR) routes.

Modes

BGP configuration mode.

Usage Guidelines

Use this command to cause the device to list itself as the next hop in updates that are sent to the specified neighbor.

Use the `no` form of this command to remove this configuration at BGP level.

Examples

The following example configures the device to list itself as the next hop in updates sent to a neighbor with the IP address 10.157.22.26.

```
device# config
device(config)# router bgp
device(config-bgp-router)# neighbor 10.157.22.26 next-hop-self
```

The following example configures the device to list itself as the next hop in updates sent to a neighbor that is a route-reflector client of the device.

```
device# config
device(config)# router bgp
device(config-bgp-router)# neighbor 10.157.22.26 next-hop-self always
```
**next-hop-mpls**

Configures BGP shortcuts using next-hop MPLS to force BGP to use an MPLS tunnel as the preferred route to a destination network when an MPLS LSP tunnel is available.

**Syntax**

```plaintext
next-hop-mpls [ compare-lsp-metric | follow-igp ]
no next-hop-mpls [ compare-lsp-metric | follow-igp ]
```

**Command Default**

BGP uses the default BGP decision process and native IP forwarding to build BGP EMCP routes. Only IP routing tables are used to resolve routes for the routing table.

**Parameters**

- **compare-lsp-metric**
  Enables BGP to compare the configured LSP metrics as the IGP cost for the next hop.

- **follow-igp**
  Ignores the MPLS metric cost in the BGP decision process and uses the IGP cost. BGP checks when an MPLS LSP is present, and totally ignores the LSP metric.

**Modes**

BGP address-family IPv4 unicast configuration mode

**Usage Guidelines**

When the `next-hop-mpls` command is enabled without either option, BGP sets the LSP metrics to one.

Enabling or disabling an option takes effect immediately. BGP automatically recalculates the existing BGP routes.

The `compare-lsp-metric` and `follow-igp` options are mutually exclusive.

When the `compare-lsp-metric` option is configured and you change the LSP metric, the routing table is updated.

Use the `no` form of the command to disable global next-hop MPLS.

When you use the `no` form of the command with the `compare-lsp-metric` or `follow-igp` option, all LSP metrics become equal cost. However, global next-hop MPLS remains enabled.

For the `follow-igp` option, consider the following:

- When you are running IGP throughout the network, and the IGP metric is trusted in the entire domain, you may want to rely on this IGP metric to make a best path and forwarding decision, regardless of whether the forwarding happens in native IP or MPLS encapsulation.

- The MPLS metric is manually configured in each LSP. There is no dynamic way to tie MPLS metric with an IGP metric. When using MPLS LSP as a BGP route outgoing interface, you loses the ability to tie the forwarding decision with a unified IGP metric.
When combined with the BGP `install-igp-cost` command, you can change the route cost from BGP MED to IGP cost and is used when BGP routes are added to the RTM.

When combined with a BGP outbound policy for route `set metric-type internal` command, you can set Layer-3 VPN and IP over MPLS routes using IGP metric to send out as the BGP MED value.

**Examples**

The following example enables BGP shortcuts through next-hop MPLS and BGP to set the next hop IGP cost to one instead of the actual LSP metric.

```bash
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# next-hop-mpls
```

The following example enables BGP shortcuts through next-hop MPLS and BGP to use the configured LSP metrics as the IGP cost for the next hop.

```bash
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# next-hop-mpls compare-lsp-metric
```

The following example enables BGP shortcuts through next-hop MPLS and BGP to ignore the LSP metrics and to use the IGP cost for the next hop.

```bash
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# next-hop-mpls follow-igp
```
**non-preempt-mode (VRRP)**

Disables preempt mode for a Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) backup device.

**Syntax**

```
non-preempt-mode
no non-preempt-mode
```

**Command Default**

Preemption is enabled by default.

**Modes**

VRID interface configuration mode

**Usage Guidelines**

This command is supported in VRRP and VRRP-E. When the `non-preempt-mode` command is entered, a backup device with a higher VRRP priority is prevented from taking control of the virtual router ID (VRID) from another backup device that has a lower priority, but has already assumed control of the VRID. Disabling preemption is useful to prevent flapping when there are multiple backup devices and a backup with a lower priority assumes the role of master. When other backup devices with a higher priority are back online, the role of master can flap between devices.

In VRRP, the owner device always assumes the role of master when it comes back online, regardless of the preempt mode setting.

Enter `no non-preempt-mode` to re-enable preemption.

**Examples**

The following example disables preempt mode for the virtual-router ID 1 session:

```
device(config)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.3/24
device(config-if-e1000-1/5)# ip vrrp vrid 1
device(config-if-e1000-1/5-vrid-1)# non-preempt-mode
```
ocsp-url
Sets the Online Certificate Status Protocol (OCSP) URL name to determine the revocation state of a certificate.

Syntax
ocsp-url URL name
no ocsp-url URL name

Parameters
URL name
The OCSP URL name.

Modes
PKI trustpoint configuration mode.

Usage Guidelines
The no form of the command removes the OCSP URL name.

Examples
The following example specifies the OCSP URL name as provided here.

device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# ocsp-url http://WIN-HJ98AK136A0.englab.brocade.com/ocsp

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
openflow controller source-interface

Configures a source-interface for the connection from the device to the controller.

Syntax

```
openflow controller source-interface { ethernet slot/port | loopback number | ve number } force-reconnect
no openflow controller source-interface { ethernet slot/port | loopback number | ve number } force-reconnect
```

Command Default

The CLI command is applicable only when the device is in active mode. The device initiates connection to the remote OpenFlow controller.

Parameters

- **ethernet slot port**
  - Gives information about a particular slot and port in an internet
- **loopback number**
  - Specifies a loopback interface.
- **ve number**
  - Specifies a virtual interface.
- **force-reconnect**
  - Forces the existing connections to use the newly configured source-interface.

Modes

Privileged EXEC mode

Usage Guidelines

When adding a new controller to the device, a connection will be attempted to the controller IP address using the configured source-interface. If the source-interface has no IP address configured or the interface is down, the syslog messages will be generated and a connection attempt will be made again in 15 seconds.

Examples

To see the source-interface, use this command.

```
device(config)#openflow controller ?
ip-address     Set the Controller IPv4 address
passive         Configure passive connection mode
source-interface Set the Source Interface to be used for controller connections
```

If a new controller is added after this, routing table will be used to connect to the controller.

```
Device(config)#openflow controller source-interface ?
ethernet        Ethernet interface
loopback        Loopback interface
ve              Virtual Ethernet interface
```
For a specified ethernet interface, use this command.

device(config)#openflow controller source-interface ethernet 2/27
force-reconnect Force the existing connections to use the newly configured source-interface

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**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**

Interface configuration mode.

**Usage Guidelines**

In interface configuration mode, this command enables Layer 2 or Layer 3 matching mode for flows with an optional enabling of hybrid port-mode.

**NOTE**

OpenFlow must be globally enabled before the Layer 2 or Layer 3 matching modes can be specified.

**Examples**

After OpenFlow 1.3 is enabled, the following example configures Layer 2 and Layer 3 matching mode for flows.

```
device# configure terminal
device(config)# openflow enable ofv130
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# openflow enable layer 23
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was modified to display OpenFlow hybrid port mode information.</td>
</tr>
</tbody>
</table>
**openflow hello-reply disable**

Allows the second Hello message (Hello-reply) to be disable on the OpenFlow Controller.

**Syntax**

```
openflow hello-reply disable
```

**Command Default**

This command needs to be run and saved when connecting to the OpenFlow Controller and any other controllers by default.

**Modes**

- EXEC and Privileged EXEC mode
- Global configuration mode

**Usage Guidelines**

When the OpenFlow Controller receives the Hello message that the controller sent, it replies with another Hello message using the same transaction-ID as in the received Hello message.

**Examples**

```
device(config)# openflow ?
controller Configure controller
default-behavior Default forwarding for no match packets
enable Enable/disable OpenFlow
hello-reply Configure HELLO Reply for HELLO originated from Controller

device(config)# openflow hello-reply ?
disable Disable HELLO Reply from the switch/router

device(config)# openflow hello-reply disable ?

device# show openflow
Administrative Status: Enabled
SSL Status: Enabled
Source-Interface: Not Configured
Source-Interface Status: NA

Controller Type: ofv130
HELLO Reply: disabled
Number of Controllers: 2

……

device# show running-config | i openflow
openflow enable ofv130
openflow hello-reply disable
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>NI05.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**org-name**

Configures the organization name for the Public Key Infrastructure (PKI) entity.

**Syntax**

```
org-name string
```

**Parameters**

`string`

Specifies name of the organization for the PKI entity.

**Modes**

PKI entity configuration mode.

**Examples**

The following example configures the organization for PKI entity.

```
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# org-name Brocade
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
org-unit-name

Configures the unit name of the organization to which the Public Key Infrastructure (PKI) entity belongs to.

Syntax

```
org-unit-name string
```

Parameters

```
string
```

Specifies unit name of the organization for PKI entity.

Modes

PKI entity configuration mode.

Examples

The following example configures unit of the organization the PKI entity belongs to.

```
device configure terminal
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# org-unit-name routing
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
owner
Designates a virtual router as the Virtual Router Redundancy Protocol (VRRP) owner and configures priority and track values.

Syntax
owner [ priority value ] [ track-priority value ]
no owner [ priority value ] [ track-priority value ]

Command Default
No virtual routers are designated as the VRRP owner.

Parameters
priority value
Abdicates owner status by setting a value that is lower than the backup default priority value. Value can be from 1 to 254. Default is 100.

track-priority value
Sets the priority value if the tracked port fails. Value can be from 1 to 254. Default is 2.

Modes
VRID interface configuration mode

Usage Guidelines
This command specifies that the device on which it is configured owns the IP address that is associated with the virtual router; making this device the default VRRP master router with its priority set to 255.

This command must be entered before the ip-address command can be configured for a VRRP virtual router ID (VRID).

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

Examples
The following example configures the device as the VRRP owner.

device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
The following example configures the device as the VRRP owner and sets the track priority to 10.

device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# owner track-priority 10
device(config-if-e1000-1/6-vrid-1)# ip-address 10.53.5.1
device(config-if-e1000-1/6-vrid-1)# activate
permit (arp-guard-access-list)

Specifies the required set of ACL rules and filters for an associated ARP guard group.

Syntax

```
permit vlan-id src-ip-address [ src-mac-address | any ]
no permit vlan-id src-ip-address [ src-mac-address | any ]
```

Command Default

If this command is not entered, no ACL rules or filters are associated with an ARP guard group.

Parameters

- `vlan-id`
  Specifies a VLAN ID in the range between 1 and 4090.

- `src-ip-address`
  Specifies a source IP address.

- `src-mac-address`
  Specifies a source MAC address.

- `any`
  Specifies all addresses.

Modes

ARP-Guard access-list name mode.

Usage Guidelines

The no form of the command removes the rules and filters for the specific ARP guard group.

Examples

The following command example specifies the required set of ACL rules and filters for the AS201 ARP guard group.

```
device# configure terminal
device(config)# arp-guard-access-list AS201
device(config-arp-guard-access-list-AS201)#permit 100 1.2.3.4 1111.2222.3333
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
pim neighbor-filter
filters the neighbor routers on an interface.

Syntax

```
[ ip | ipv6 ] pim neighbor-filter aclname
no [ ip | ipv6 ] pim neighbor-filter aclname
```

Parameters

- **acl name**: Filters neighbor to participate in PIM.

Modes

- Global configuration mode.
- EXEC mode.
- Privileged EXEC mode.

Command Output

The `pim neighbor-filter` command is used on an interface to filter the neighbor routers.

Examples

```
device configure terminal
device(config)# interface ethernet 1/3
device(config-if-e1000-1/3)# ip pim neighbor-filter 10
device(config-if-e1000-1/3)# ipv6 pim neighbor-filter f10
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was added to filter the neighbor router on the interface.</td>
</tr>
</tbody>
</table>
**ping mpls ldp**

Sends an MPLS echo request from the ingress to the egress LSR.

**Syntax**

```plaintext
ping mpls ldp { ip_addr | ip_addr/mask_length } [ count num | destination ip_addr | detail | nexthop ip_addr | reply-mode
 [ no_reply | router_alert ] ] reply-tos num | size bytes | source ip_addr | timeout msec ]
```

**Parameters**

- `ip_addr`
  Specifies the LDP IPv4 FEC destination prefix.

- `ip_addr/mask_length`
  Specifies the LDP IPv4 destination prefix and mask length. If the mask-length is not specified, the default value is 32.

- `count num`
  Specifies the number of echo requests to send. Values are from 1 to 4294967294. The default value is five.

- `destination ip_addr`
  Specifies an IP address within the 127/8 subnet. The default address is 127.0.0.1.

- `detail`
  Displays the details of the echo request and reply messages. By default, the display is in the brief mode.

- `nexthop ip_addr`
  The next closest router a packet can go through. The nexthop IPv4 address to send the OAM request to. If an address that does not match the outgoing path for the tunnel is given, following error message appears as the response: `Ping fails: LDP next-hop does not exist`.

- `reply-mode`
  Specifies the reply mode field in the echo request only if the user does not want the reply to be sent as an IPv4 UDP packet.

  - `no_reply`
    Use to test one-way connectivity.

  - `router_alert`
    Use when the normal IP return path is unreliable. This option indicates that the reply must be sent as an IPv4 UDP packet with the Router Alert option. This option requires extra overhead processing at each LSR along the return path.

- `reply-tos num`
  Specifies a TOS value between 0 and 254 to include in the Reply-TOS-byte TLV. By default, the reply-tos TLV is not included in the echo request. The last bit of the TOS byte is always 0.

- `size bytes`
  Specifies that the size of the echo request, including the label stack, to send. The pad TLV is used to fill the echo request message to the specified size. The minimum packet size is 80 bytes for an LDP echo request. The maximum packet size is the size of the LSP MTU.

- `source ip_addr`
Specifies the IP address of any interface. Use this address as the destination address for the echo reply address. The default address is the LSR ID.

**timeout msec**

Specifies an interval in milliseconds for the echo request message. The value range is from 50 to 300000. The default timeout is 5 seconds. The maximum timeout value is 5 minutes.

**Modes**

Global configuration mode.

**Usage Guidelines**

**NOTE**

Once an outgoing path is chosen to send the ping request, it is not changed. Disabling the path does not cause the ping packet to be sent over other ECMP paths. Upon disabling the path, the ping operation stops because the path is down. This is the expected behavior.

**Examples**

The following example displays how to perform the LSP LSP ping operation.

```
device# ping mpls ldp 10.22.22.22
Send 5 80-byte MPLS Echo Requests for LDP FEC 10.22.22.22/32, timeout 5000 msec
Type Control-c to abort
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max=0/1/1 ms.
device#
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td><strong>next-hop ipv4-address</strong> is added to the existing ping command.</td>
</tr>
</tbody>
</table>
pki authenticate
Configures authentication for the CA.

Syntax
pki authenticate trustpoint-name

Parameters
trustpoint-name
Specifies trustpoint name.

Modes
Global configuration mode.

Usage Guidelines
This command authenticates the CA by obtaining the self-signed certificate of the CA that contains the public key of the CA. Since the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator before you run this command. This command is saved to the router configuration and the certificates are saved to the router.

Examples
The following example configures authentication for the CA.

device configure terminal
device(config)# pki authenticate brocade

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**pki cert validate**

Validates or checks if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid.

**Syntax**

```
pki cert validate trustpoint-name
```

**Parameters**

```
trustpoint-name
```

Specifies the trustpoint name.

**Modes**

Global configuration mode.

**Usage Guidelines**

Use this command after loading the router certificate using the `import` command to validate the router certificate.

The following files must be downloaded first to the MP flash drive using TFTP and then imported into the system software using the `import` command:

- CA/trustpoint certificate
- Router certificate
- Router private key

**Examples**

The following example configures validation of a trustpoint.

```
device(config)# pki cert validate brocade
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
pki enroll
Generates a certificate request that is sent to the specified CA trustpoint. This enrolls the router on the CA trustpoint.

Syntax
pki enroll name

no pki enroll name

Command Default
By default, this command is not configured.

Parameters
name
Specifies the CA trustpoint to which the router sends the request for certificates.

Modes
Global configuration mode

Usage Guidelines
Use the no form of this command to remove the certificates from the router.
The requested certificates are added to each key pair of your router.
The requested certificates are saved to the router, but the command is not.

Examples
This example generates a certificate request that is sent to the CA trustpoint named mytrustpoint.

device(config)# pki enroll mytrustpoint

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**pki entity**

Configures the Public Key Infrastructure (PKI) end-user parameters and enters the PKI entity configuration mode.

**Syntax**

```
pki entity name
```

**Parameters**

`name`

Specifies entity name for the PKI entity.

**Modes**

Global configuration mode.

**Examples**

The following example configures the PKI entity and enters the PKI entity configuration mode.

```
device configure terminal
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)#
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**pki export**
Manually exports certificates from the specified CA trustpoint to the flash memory of the router. Export certificates after the router is rebooted to ensure the router has current, valid certificates.

**Syntax**

```
pki export name pem url filename
```

**Command Default**
By default, this command is not configured.

**Parameters**

- **name**
  Specifies the name of the CA trustpoint that has the certificates you want to export to the flash memory of the router.

- **pem url filename**
  Specifies the name of the file being exported to the flash memory of the router. The file contains the certificates.

**Modes**
Privileged EXEC mode

**Usage Guidelines**

**NOTE**
The trustpoint name you specify must match the name of the trustpoint you specified using the `pki trustpoint` command.

Use the `pki export key` command to manually export key-pairs to the router, or the `pki export crl` to manually export certificate revocation lists to the router.

**Examples**

This example manually exports certificates from the CA trustpoint named `mytrustpoint` to the flash memory of the router. The exported file that contains the certificates is named `file1certs`.

```
device# pki export mytrustpoint pem url file1certs
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
pki export crl

Manually exports certificate revocation lists (CRL) from the specified CA trustpoint to the flash memory of the router. Export the CRL after the router is rebooted to ensure the router has current, valid lists.

Syntax

```
pki export crl trustpointname url filename
```

Command Default

By default, this command is not configured.

Parameters

- **trustpointname**: Specifies the name of the CA trustpoint that has the CRL you want to export to the flash memory of the router.
- **url filename**: Specifies the name of the file being exported to the flash memory of the router. The file contains the CRL.

Modes

Privileged EXEC mode

Usage Guidelines

**NOTE**
The trustpoint name you specify must match the name of the trustpoint you specified using the `pki trustpoint` command.

Use the `pki export` command to manually export certificates to the router, or the `pki export key` command to manually export key-pairs to the router.

Examples

This example manually exports CRL from the CA trustpoint named `mytrustpoint` to the flash memory of the router. The exported file that contains the CRL is named `filecrl`.

```
device# pki export crl mytrustpoint url filecrl
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
pki export key

Manually exports key-pairs from the specified CA trustpoint to the flash memory of the router. Export key-pairs after the router is rebooted to ensure the router has current, valid key-pairs.

Syntax

\texttt{pki export key label password filename}

Command Default

By default, this command is not configured.

Parameters

\texttt{label}

Specifies the label (name) of the key-pair being exported to the flash memory of the router.

\texttt{password}

Specifies the password required to export key-pairs.

\texttt{filename}

Specifies the name of the file being exported to the flash memory of the router. The file contains the key-pair.

Modes

Privileged EXEC mode

Usage Guidelines

Use the \texttt{pki export} command to manually export certificates to the router, or the \texttt{pki export crl} command to manually export CRL to the router.

Examples

This example manually exports the key-pair labeled 1212 from the CA trustpoint named \texttt{mytrustpoint} to the flash memory of the router. The exported file that contains the key-pair is named \texttt{file1key}, and the password is \texttt{password}.

\texttt{device# pki export 1212 password file1key}

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**pki import**

Manually imports certificates from the flash memory of the router to the specified CA trustpoint.

**Syntax**

```
pki import name { pem | url flash: file-name }
```

**Command Default**

By default, this command is not configured.

**Parameters**

- **name**
  Specifies the name of the CA trustpoint that receives the certificates being imported from the router.

- **pem**
  (Optional) Specifies the name of the .pem file to be imported. The file contains the certificates.

- **url flash: file-name**
  (Optional) Specifies the name of the flash file to be imported. The file contains the certificates.

**modes**

Global configuration mode

**Usage Guidelines**

**Examples**

The following example manually imports certificates to the CA trustpoint named `brocade`.

```
device(config)# pki import brocade pem url flash: mlx2.crt
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**pki import key ec**

Enables importing the Elliptic Curve (EC) key pair from the flash file with the specified key label.

**Syntax**

```
pki import key ec key-label pem url flash: file-name
no pki import key ec key-label pem url flash: file-name
```

**Parameters**

- **key-label**
  Specifies the key label name.

- **pem**
  Specifies .pem file name used to import.

- **url flash: file-name**
  Specifies the flash file name.

**Modes**

Global configuration mode.

**Usage Guidelines**

The `no` form of the command cancels the import request that was enabled earlier.

**Examples**

The following example enables importing the EC key pair from the flash file with the specified key label.

```
device(config)# pki import key ec brocade pem url flash: mlx2_eckey.pem
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**pki profile-enrollment**

Creates a PKI enrollment profile you can use to efficiently enroll requester systems. Systems you enroll using the profile have the same You name the profile and specify the profile settings using command parameters.

**Syntax**

```
pki profile-enrollment name authentication-url url-string authentication-command url-string enrollment-url url-string password
no pki profile-enrollment name authentication-url url-string authentication-command url-string enrollment-url url-string password
```

**Command Default**

By default, this command is not configured.

**Parameters**

- `name`
  
  Specifies the name of the enrollment profile.

- `authentication-url url-string`
  
  Specifies the URL of the certification authority (CA) server you want to receive the authentication requests. Make sure you use the correct form of the URL.

- `authentication-command string`
  
  Specifies the HTTP command that is sent to the certification authority (CA) for authentication.

- `enrollment-url url-string`
  
  Specifies the URL of the certification authority (CA) server you want to receive the enrollment requests. Make sure you use the correct form of the URL.

- `password`
  
  Specifies the password for the SCEP challenge used to revoke the requester's current certificate and issue another certificate for auto mode. Copy the password from the server.

**Modes**

- Global configuration mode (to enter the command)
- Pki-profile mode (to specify parameter values)

**Usage Guidelines**

Use the `no` form of this command to delete all information defined in the enrollment profile.

Entering the `pki profile-enrollment` command automatically enters pki-profile mode, which is required to specify the command parameter values.

**NOTE**

You must specify the authentication and enrollment URLs in the correct form. The URL argument must be in the form `http://CA_name`, where CA_name is the host Domain Name System (DNS) name or the IP address of the CA.
Examples

This example creates an enrollment profile named profileA. The values for the parameters are:

- **authentication-url**: http://win-ab12aaa123a1.lab.myco.com/CertServer/mscep/mcse
- **authentication-command**: win-as12aaa123a1.lab.myco.com.lab-WIN-A1B1A1BBBB
- **enrollment-url**: http://win-ab12aaa123a1.lab.myco.com/CertServer/mscep/mscep
- **password**: 1B1111AB111A2222

```
device(config)# pki profile-enrollment profileA
device(config-pki-profile)# authentication-url http://win-ab12aaa123a1.lab.myco.com/CertServer/mscep/mcse
device(config-pki-profile)# authentication-command win-as12aaa123a1.lab.myco.com.lab-WIN-A1B1A1BBBB
device(config-pki-profile)# enrollment-url http://win-ab12aaa123a1.lab.myco.com/CertServer/mscep/mscep
device(config-pki-profile)# 1B1111AB111A2222
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**pki trustpoint**

Configures the trustpoint used in all the relevant parameters needed for communication and enters the Public Key Infrastructure (PKI) trustpoint configuration mode.

**Syntax**

```
pki trustpoint name
no pki trustpoint name
```

**Parameters**

name

Specifies the PKI trustpoint name.

**Modes**

Global configuration mode.

**Usage Guidelines**

The `no` form of the command deletes all the certificates associated with this Certificate Authority (CA). The trustpoint can be a self-signed root CA or a subordinate CA.

**Examples**

The following example configures the PKI trustpoint and enters the PKI trustpoint configuration mode.

```
device configure terminal
device(config)# pki trustpoint brocade
device(config-pki-trustpoint-brocade)#
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
pki-entity

Configures the Public Key Infrastructure (PKI) entity parameter to be used while enrolling to a CA.

Syntax

```
pki-entity entity-name
```

Parameters

- `entity-name`
  Specifies the entity name for the PKI entity.

Modes

PKI trustpoint configuration mode.

Examples

The following example configures the PKI entity and enters the PKI trustpoint configuration mode.

```
device configure terminal
device(config)# pki trustpoint brocade
device(config-pki-trustpoint-brocade)# pki-entity brocade-entity
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
port

Adds member ports to the transparent VLAN flooding (TVF) domain.

Syntax

port ethernet slot/port { to slot/port | [ ethernet slot/port to slot/port | ethernet slot/port ] ... ]
no port ethernet slot/port { to slot/port | [ ethernet slot/port to slot/port | ethernet slot/port ] ... ]

Command Default

The TVF domain does not have member ports.

Parameters

ethernet slot/port

Specifies an Ethernet interface to be added to the TVF domain.

to slot/port

Specifies a range of Ethernet interfaces to be added to the TVF domain.

Modes

TVF domain configuration mode

Usage Guidelines

The number of ports in the LAG that can be added to the TVF domain is limited based on the maximum FID pool size configured using the `system-max tvf-lag-ib-fid-group` command.

The `no` form of the command removes the member ports added to the TVF domain.

Examples

The following example adds member ports to the TVF domain.

device# configure terminal
device(config)# tvf-domain 1
device(config)# port ethernet 1/1 ethernet 2/1

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
pre-shared-key

Configures the pre-shared MACsec key on the interface.

Syntax

```
pre-shared-key key-id key-name name
no pre-shared-key key-id key-name name
```

Command Default

No pre-shared MACsec key is configured on the interface.

Parameters

- **key-id**
  Specifies the Connectivity Association Key (CAK) key value. Key-id must be hexadecimal string of 32 characters.

- **name**
  Specifies the Connectivity Association Key (CAK) key name. Key-name must be hexadecimal string of maximum 64 characters.

Modes

```
dot1x-mka-interface mode.
```

Usage Guidelines

The pre-shared key is required for communications between MACsec peers.

**NOTE**

1. Group must be attached to the interface before applying pre-shared key on the interface.
2. Key-name length should be multiple of 4.
3. Key-name and pre-shared key must be hexadecimal string.

The `no` form of the command removes the pre-shared key from the interface.

Examples

The following example configures pre-shared key with a name beginning with 11223344 and with the value shown, to port 1, slot 1 on the device.

```
device configure terminal
device(config)# dot1x-mka-enable
device(config-dot1x-mka)# enable-mka ethernet 1/1
device(config-dot1x-mka-eth-1/1)# pre-shared-key 0102030405060708090A0B0C0D0E0F10 key-name 11223344
```
# History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**preforwarding-time**

Configures the preforwarding time interval, the time a port will remain in the preforwarding state before changing to the forwarding state.

**Syntax**

```
preforwarding-time milliseconds
no preforwarding-time milliseconds
```

**Command Default**

The default preforwarding time interval is 300 milliseconds.

**Parameters**

*milliseconds*

The preforwarding time interval in milliseconds. The range is from 200 through 30000 milliseconds.

**Modes**

MRP configuration mode

**Usage Guidelines**

The preforwarding time interval must be at least twice the value of the hello time or a multiple of the hello time.

When MRP is enabled, all ports begin in the preforwarding state.

An interface changes from the preforwarding state to the forwarding state when the port preforwarding time expires. This occurs if the port does not receive a Ring Health Packet (RHP) from the master, or if the forwarding bit in the RHPs received by the port is off (indicating a break in the ring). The port heals the ring by changing its state to forwarding. If a member port in the preforwarding state does not receive an RHP within the preforwarding time, the port assumes that a topology change has occurred and changes to the forwarding state.

The secondary port on the master node changes to the blocking state if it receives an RHP, but changes to the forwarding state if the port does not receive an RHP before the preforwarding time expires. A member node preforwarding interface also changes from preforwarding to forwarding if it receives an RHP whose forwarding bit is on.

If Unidirectional Link Detection (UDLD) is also enabled on the device, Brocade recommends that you set the MRP preforwarding time slightly higher than the default of 300 ms; for example, to 400 or 500 ms.

The `no` form of the command sets the preforwarding time interval to the default.

**Examples**

The following example shows how to configure the preforwarding time to 400 milliseconds.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-1)# preforwarding-time 400
```
prf

Configures a pseudorandom function (PRF) for an Internet Key Exchange version 2 (IKEv2) proposal.

Syntax

prf { sha256 | sha384 }
no prf { sha256 | sha384 }

Command Default

The default algorithm is SHA-384.

Parameters

sha256
Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.

sha384
Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.

Modes

IKEv2 proposal configuration mode

Usage Guidelines

This hash algorithm is used to generate key material during IKEv2 SA negotiations.

Both algorithms may be configured for an IKEv2 proposal.

When only one PRF algorithm is configured for an IKEv2 proposal, removing it restores the default configuration.

The no form of the command removes the specified PRF algorithm configuration.

Examples

The following example shows how to configure SHA-256 as the hash algorithm for an IKEv2 proposal named ikev2_prop.

device(config)# ikev2 proposal ikev2_prop
device(config-ikev2-proposal-ikev2_prop)# prf sha256

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**protected**

Configures VRF traffic protection for an Internet Key Exchange version 2 (IKEv2) profile.

**Syntax**

```
protected vrf
no protected vrf
```

**Parameters**

- `vrf`
  
  Specifies the name of the VRF to be protected.

**Modes**

IKEv2 profile configuration mode

**Usage Guidelines**

When the tunnel VRF and the protected VRF do not match, an IKEv2 session is not initiated.

The `no` form of the command removes the specified VRF traffic protection configuration for the IKEv2 profile.

**Examples**

The following example shows how to configure an IKEv2 profile named test to protect traffic for a VRF named red.

```
device(config)# ikev2 profile test
device(config-ikev2-profile-test)# protected red
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**radius-server host**

Configures the Remote Authentication Dial-In User Service (RADIUS) server.

**Syntax**

```
radius-server host { ipv4-address | host-name | ipv6-address} [ auth-port port-num [ acct-port port-num [ { accounting-only | authentication-only | default } [ ssl-auth-port port-num [ { accounting-only | authentication-only | default } [ key key-string | dot1x ] ] ] ] ] ]
```

```
no radius-server host { ipv4-address | host-name | ipv6-address} [ auth-port port-num [ acct-port port-num [ { accounting-only | authentication-only | default } [ ssl-auth-port port-num [ { accounting-only | authentication-only | default } [ key key-string | dot1x ] ] ] ] ] ]
```

**Command Default**

The RADIUS server host is not configured.

**Parameters**

- **ipv4-address**
  
  Configures the IPv4 address of the RADIUS server.

- **host-name**
  
  Configures the host name of the RADIUS server.

- **ipv6-address**
  
  Configures the IPv6 address of the RADIUS server.

- **auth-port port-num**
  
  Configures the authentication UDP port. The default value is 1812.

- **acct-port port-num**
  
  Configures the accounting UDP port. The default value is 1813.

- **accounting-only**
  
  Configures the server to be used only for accounting.

- **authentication-only**
  
  Configures the server to be used only for authentication.

- **default**
  
  Configures the server to be used for any AAA operation.

- **key key-string**
  
  Configures the RADIUS key for the server.

- **dot1x**
  
  Configures support for EAP for 802.1X.

- **ssl-auth-port port-num**
  
  Specifies that the server is a RADIUS server running over a TLS-encrypted TCP session. Only one of auth-port or ssl-auth-port can be specified. If neither is specified, it defaults to the existing default behavior, which uses the default
auth-port of 1812 and 1813 for accounting with no TLS encryption. The default destination port number for RADIUS over TLS is TCP/2083. There are no separate ports for authentication, accounting, and dynamic authorization changes. The source port is arbitrary.

**accounting-only**
Configures the server to be used only for accounting.

**authentication-only**
Configures the server to be used only for authentication.

**default**
Configures the server to be used for any AAA operation.

### Modes
Global configuration mode

### Usage Guidelines
Use the `radius-server host` command to identify a RADIUS server to authenticate access to a Brocade device. You can specify up to eight servers. If you add multiple RADIUS authentication servers to the Brocade device, the device tries to reach them in the order you add them. To use a RADIUS server to authenticate access to a Brocade device, you must identify the server to the Brocade device. In a RADIUS configuration, you can designate a server to handle a specific AAA task. For example, you can designate one RADIUS server to handle authorization and another RADIUS server to handle accounting. You can specify individual servers for authentication and accounting, but not for authorization. You can set the RADIUS key for each server.

The `no` form of the command removes the configuration.

### Examples
The following example shows how to configure a RADIUS server to authenticate access to a Brocade device.

```
device(config)# radius-server host 192.168.10.1
```

The following example shows how to specify different RADIUS servers for authentication and accounting.

```
device(config)# radius-server host 10.2.3.4 auth-port 1800 acct-port 1850 default key abc
device(config)# radius-server host 10.2.3.5 auth-port 1800 acct-port 1850 authentication-only key def
device(config)# radius-server host 10.2.3.6 auth-port 1800 acct-port 1850 accounting-only key ghi
```

The following example shows how to map the 802.1X port to a RADIUS server.

```
device(config)# radius-server host 10.2.3.4 auth-port 1800 acct-port 1850 default key abc dot1x
```
rate-limit input

Configures the per-port or port per VLAN broadcast, unknown-unicast, or multicast (BUM) rate-limiting.

Syntax

```
rate-limit input [ vlan vlan-id ] [ broadcast | unknown-unicast | multicast ] [ average-rate maximum burst size ] [ include-control ] [ shutdown timeout ] [ alert high-watermark low-watermark ]
```

Parameters

- **vlan vlan-id**
  Specifies the VLAN id of the specific port on which the rate-limiting of BUM traffic is accounted.

- **broadcast unknown-unicast multicast**
  Define a rate limit for ingress broadcast, unknown-unicast, or multicast packets on the port. Any combination of these parameters can be used to define the rate limit.

- **average-rate**
  Specifies the maximum number of bits a port is allowed to receive during a one-second interval and is the aggregate sum of the broadcast, unknown-unicast, and multicast packets rate limit, if the rate limit is configured for all three packets. The software automatically adjusts the number you enter to the nearest multiple of 8,144 bits per second (bps).

- **maximum burst size**
  Specifies the value of the maximum burst of traffic allowed by the specific port.

- **include-control**
  Extends the existing BUM rate-limit to include rate limit of ARP, other control packets.

- **shutdown timeout**
  Specifies that the port is to be shut down if the amount of BUM traffic exceeds the pre-defined limit. Time out value is between 0 to 1440 minutes.

- **alert high-watermark low-watermark**
  Alert message if the rate crossed over/under limit shutdown. Shut down the port if the rate is over limit.

Modes

- Interface configuration mode

Usage Guidelines

Examples

The following is an example for rate-limit input configuration.

```
device(config)#int eth 1/1
device(config-if-e1000-1/1)#rate-limit input broadcast 100000 10000 include-control shutdown 1 alert 80000 10000
device(config-if-e1000-1/1)#rate-limit input multicast 100000 10000 include-control shutdown 1 alert 80000 10000
```
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 05.7.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 05.9.00</td>
<td>This command was modified to include the <strong>include-control</strong> option.</td>
</tr>
</tbody>
</table>
rd

Each instance of a VRF must have a unique Route Distinguisher (RD) assign to it.

Syntax

rd \{ as-num:id | ip-num:id \}
no rd \{ as-num:id | ip-num:id \}

Command Default

No RD is assigned to the VRF.

Parameters

as-num:id

Composed of the local ASN number followed by a colon ":" and a unique arbitrary number. For example 3:6.

ip-num:id

Composed of the local IP address followed by a colon ":" and a unique arbitrary number.

Modes

VRF configuration mode

Usage Guidelines

Each instance of a VRF must have a unique Route Distinguisher (RD) assigned to it. The RD is pre-pended to any address being routed or advertised. The RD can be defined as either ASN relative or IP address relative. Because the RD is unique to an instance of a VRF, it allows the same IP address to be used in different VPNs without creating any conflict.

The no form of the command returns to the default setting.

Examples

The following example displays the command which assigns a Route Distinguisher (RD) based on the AS number 3 and the arbitrary identification number 6.

device(config-vrf)# rd 3:6
**remove-tagged-ports / remove-untagged-ports**

Removes tagged or untagged ports on the VLAN.

**Syntax**

```plaintext
remove-tagged-ports
remove-untagged-ports
```

**Command Default**

None.

**Modes**

VLAN configuration mode (config-vlan).

**Examples**

The following example displays the remove-tagged-ports command.

```plaintext
device(config-vlan-100)# remove-tagged-ports
Vlan : 100, Ports removed : ethe 1/1 to 1/2 ethe 4/1 to 4/8
device(config-vlan-100)#
```

The following example displays the remove-untagged-ports command.

```plaintext
device(config-vlan-100)# remove-untagged-ports
Vlan : 100, Ports removed : ethe 3/1 to 3/24
device(config-vlan-100)#
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
**remove-vlan**

Removes tagged and untagged ports from all or defined VLANs.

**Syntax**

```
remove-vlan [ all | vlan [ vlan_id ] ] { to vlan_id }
```

**Parameters**

- **all**
  - Removes all configured VLANs.

- **vlan vlan_id**
  - Specifies the VLAN where the ports should be removed.

- **to vlan_id**
  - Specifies the VLAN range to remove.

**Modes**

User configuration level.

**Examples**

The following example displays the command with the `all` option.

```
device(config-if-e100000-1/1)# remove-vlan all
Port ethe 1/1  removed from tagged vlan : 300 400 500 600 700 800 900 1000 2000 3000 4000  and untagged
    vlan : 200 .
device(config-if-e100000-1/1)#
```

The following example displays the command with a specified VLAN range.

```
device(config-if-e100000-1/2)# remove-vlan vlan 2 to 4090
Port ethe 1/2  removed from tagged vlan : 300 400 500 600 700 800 900 1000 2000 3000 4000  and untagged
    vlan : 200 .
device(config-if-e100000-1/2)#
```

The following example displays the command that remove a specific VLAN.

```
device(config-if-e10000-4/1)# remove-vlan vlan 500
Vlan : 500, Ports removed : ethe 4/1
device(config-if-e10000-4/1)#
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
reverse-metric

Configures the reverse metric value at the IS-IS router level.

Syntax

reverse-metric [ value ] [ whole-lan ] [ te-def-metric ]
no reverse-metric [ value ] [ whole-lan ] [ te-def-metric ]
reverse-metric tlv-type [ value ]
no reverse-metric tlv-type [ value ]

Command Default

The reverse-metric command is disabled by default.

Parameters

reverse-metric

Specifies the reverse metric parameter at the IS-IS router level.

value

Specifies the reverse metric value in metric style. The metric style consists of narrow or wide style. The narrow metric range is from 1 - 63. The wide metric range is from 1 - 16777215. The default value is 16777214 irrespective of the metric style configured. If the reverse-metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor router receives the reverse metric value through the IS hello, the neighbor router updates the cost to reach the original IS-IS router with the sum of default metric and the reverse metric value. This helps in shifting traffic to the other alternate paths.

whole-lan

Specifies changing the reverse metric parameter for the entire LAN. The whole-lan option indicates the whole LAN bit in the flag. If the whole-lan option is enabled, the configured reverse metric value affects the entire LAN. If the whole-lan option is not enabled, the reverse metric value affects only the neighbor router. This option takes effect only on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the whole-lan option is enabled.

te-def-metric

Specifies setting the TE default metric sub-TLV. If the te-def-metric option is enabled, the router sends a TE default metric sub-TLV within the reverse-metric TLV.

tlv-type value

Specifies the TLV type for the reverse metric parameter. The TLV type can only be configured at the IS-IS router level. The tlv-type value parameter must be configured in the range of unassigned IS-IS TLV values. The tlv-type value parameter should not be configured with existing IS-IS TLV types. The default value is 254.

Modes

IS-IS router level.

Usage Guidelines

Use the reverse-metric command when you are performing network maintenance operations, such as software upgrades, on an IS-IS router node. When maintenance operations are performed, the router undergoing maintenance should not be used by the neighbor routers to forward transit traffic. In order to shift traffic away from the router undergoing maintenance, configure the reverse-metric command on the maintenance router. The router undergoing maintenance first advertises a reverse metric TLV in a IS-IS hello PDU to its neighbor router on a point-to-point or multi-access link. When the neighbor router receives a high reverse metric value, the router selects alternate paths to forward traffic while maintenance is going on. The neighbor router adds the reverse metric TLV to its own TE default metric sub-TLV and recalculates its SPF tree and route topology. The
neighbor router floods the new LSP containing the extended IS reachability TLV throughout the domain. Traffic gradually shifts onto alternate paths away from the link between the maintenance router and the neighbor router as nodes in the IS-IS domain receive the new LSP. Once the maintenance is complete, you can remove the reverse-metric command configuration from the router, and the reverse metric TLV in the IS-IS hello PDU is no longer advertised to the neighbor router. The IS-IS neighbor router reverts back to its original IS-IS metric, and the traffic switches to the original IS-IS router to reach its destination.

In a multi-access link, the IS-IS DIS router adds the reverse metric TLV value to each node's default metric value in the pseudonode LSP when the whole-lan flag is set. All non-DIS nodes ignore the reverse metric TLV. If multiple neighbor routers advertise the reverse metric TLV with the whole LAN flag set, the neighbor router with the highest MAC address takes precedence, and the value advertised by that neighbor is updated in the pseudonode LSP for all neighbors. If some neighbor routers do not set the whole LAN flag, then the reverse metric TLV value advertised by the neighbor router is updated in the pseudonode LSP for that neighbor only.

The S flag is set when the sender of the reverse metric TLV signals to the neighbor router to use the TE sub-tlv for the default metric (sub-tlv type 18) in the reverse metric TLV. When the receiving router finds the S flag set in the reverse metric TLV, the router searches for the TE sub-tlv. The router adds the default metric value in the TE sub-tlv to the configured TE default metric value and recalculates the CSPF.

The no form of the command, specified with the configured value, resets the metric value to the default value of 16777214. The no reverse-metric command removes the entire reverse metric configuration.

**NOTE**
The reverse-metric value command is supported on the Brocade NetIron XMR Series, the Brocade MLX Series, and the Brocade NetIron CER Series and Brocade NetIron CES Series platforms.

**Examples**
The following example configures the reverse metric value to 50 at the router level. The whole-lan option is enabled to include the entire LAN.

```
device(config)# router isis
device(config-isis-router)# reverse-metric
device(config-isis-router)# reverse-metric 50 whole-lan
```

The following example configures the reverse metric TLV type in the range of unassigned IS-IS TLV values.

```
device(config-isis-router)# reverse-metric tlv-type
device(config-isis-router)# reverse-metric tlv-type 230
```

Use the show isis config command to display the configuration of the reverse metric value at the router level. The reverse metric value and the parameters, whole-lan and te-def-metric are highlighted in the output.

```
device(config)# show isis config
    router isis
    net 49.2211.aaaa.bbbb.cccc.00
    reverse-metric 50 whole-lan te-def-metric
    address-family ipv4 unicast
    address-family ipv6 unicast
```

NetIron Command Line Interface (CLI) Reference Guide
53-1004199-02 489
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**revocation-check**

Specifies the type of method to be followed for revocation check of the certificate authority (CA).

**Syntax**

```
revocation-check { crl | ocsp | none }
no revocation-check { crl | ocsp | none }
```

**Command Default**

Revocation check is not enabled.

**Parameters**

- **crl**
  
  Specifies the certificate revocation list (CRL) method for revocation check.

- **ocsp**
  
  Specifies the Online Certificate Status Protocol (OCSP) method for revocation check.

- **none**
  
  Specifies that none of the methods are selected for revocation check.

**Modes**

PKI trustpoint configuration mode.

**Usage Guidelines**

The `no` form of the command removes the method selected for revocation check.

**Examples**

The following example specifies the crl as the revocation check method.

```
device(config)# pki trustpoint brocade1
device(config-pki-trustpoint-brocade1)# revocation-check crl
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**rfc1583-compatibility (OSPF)**

Configures compatibility with RFC 1583.

**Syntax**

```
rfc1583-compatibility
no rfc1583-compatibility
```

**Command Default**

This command is disabled by default.

**Modes**

OSPF router configuration mode
OSPF router VRF configuration mode

**Usage Guidelines**

Enter `no rfc1583-compatibility` to disable compatibility with RFC 1583 if it has been enabled. Enter `no rfc1583-compatibility` if it has been enabled to re-enable compatibility with RFC 2328.

When this command is enabled, OSPF is compatible with RFC 1583 (OSPFv2) and OSPF prefers the least cost path to the autonomous system border router (ASBR). Disabling this compatibility causes OSPF to prefer the non-backbone area path over backbone area paths in addition to the least cost path to the ASBR.

When upgrading software from 5.8x and earlier, the device preserves the existing configuration value for OSPF RFC 1583 compatibility based on the version of the startup configuration file. New OSPF configurations use the new default value.

**Examples**

This example enables compatibility with RFC 1583.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# rfc1583-compatibility
```

This example disables compatibility with RFC 1583 if it has been enabled and re-enables compatibility with RFC 2328.

```
device# configure terminal
device(config)# router ospf
device(config-ospf-router)# no rfc1583-compatibility
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified so that it is disabled by default.</td>
</tr>
<tr>
<td>5.9.00a</td>
<td>This command was modified so that existing configurations are preserved when upgrading software.</td>
</tr>
</tbody>
</table>
ring-interface
Configures the primary and secondary interfaces for the ring to control outward traffic flow.

Syntax

```
ring-interface ethernet slot/port ethernet slot/port
no ring-interface ethernet slot/port ethernet slot/port
```

Command Default
The primary and secondary interfaces are not configured.

Parameters

- **ethernet slot/port**
  Configures the primary and secondary interfaces.

Modes

MRP configuration mode

Usage Guidelines
On the master node, the primary interface is the one that originates Ring Health Packets (RHPs). Ring control traffic and Layer 2 data traffic will flow in the outward direction from this interface by default. On member nodes, the direction of traffic flow depends on the traffic direction selected by the master node. Therefore, on a member node, the order in which you enter the interfaces does not matter.

**NOTE**
The Brocade NetIron CES and CER Series devices do not support selection of a secondary interface based on reception of RHPs. As a result, the primary and secondary interfaces must be configured correctly.

The **no** form of the command clears the primary and secondary interfaces.

Examples
The following example shows how to configure the primary and secondary interfaces on a ring.

```
device(config)# vlan 2
device(config-vlan-2)# metro-ring 1
device(config-vlan-2-mrp-2)# ring-interface ethernet 1/1 ethernet 1/2
```
**router-interface**

Configures the VE per VPLS instance.

**Syntax**

```
router-interface { ve num }
```

**Command Default**

None.

**Parameters**

- `ve num`
  
  Specifies the Virtual Ethernet interface number.

**Modes**

- MPLS VPLS sub-configuration mode (config-mpls-vpls).

**Usage Guidelines**

The user must specify a router-interface for each VPLS instance.

**Examples**

The following example displays when the user must specify a router-interface for each VPLS instance.

```
device(config)# router mpls
device(config-mpls)# vpls test 10
device(config-mpls-vpls-test)# router-interface ve 200
device(config-mpls-vpls-test)# vlan 10
device(config-mpls-vpls-test-vlan-10)# tagged ethe 4/1
device(config-mpls-vpls-test-vlan-10)# vlan 200 isid 20000
```
**router vrrp**

Globally enables Virtual Router Redundancy Protocol (VRRP).

**Syntax**

```
router vrrp
no router vrrp
```

**Command Default**

VRRP is not globally enabled.

**Modes**

Global configuration mode

**Usage Guidelines**

After globally enabling VRRP, the command prompt does not change. Nearly all subsequent VRRP configuration is performed at the interface level, but VRRP must be enabled globally before configuring VRRP instances.

The `no router vrrp` command disables VRRP globally.

**Examples**

The following example globally enables VRRP and enters interface configuration mode.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/5
```
router vrrp-extended

Globally enables Virtual Router Redundancy Protocol Extended (VRRP-E) and enters VRRP-E router configuration mode.

Syntax

- router vrrp-extended
- no router vrrp-extended

Command Default

VRRP-E is not globally enabled.

Modes

Global configuration mode

Usage Guidelines

After globally enabling VRRP-E, nearly all subsequent VRRP-E configuration is performed at the interface level. VRRP-E must be enabled globally before configuring VRRP-E instances.

The `no router vrrp-extended` command globally disables VRRP-E.

Examples

The following example globally enables VRRP-E and enters interface configuration mode.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# interface ethernet 1/5
device(config-if-e1000-1/5)# ip address 10.53.5.24/24
device(config-if-e1000-1/5)# ip vrrp-extended vrid 1
device(config-if-e1000-1/5-vrid-1)# backup priority 110
device(config-if-e1000-1/5-vrid-1)# version 2
device(config-if-e1000-1/5-vrid-1)# ip-address 10.53.5.254
device(config-if-e1000-1/5-vrid-1)# activate
VRRP-E router 1 for this interface is activating
```
rpf shortcut

Enables RPF shortcut for LSP paths.

Syntax

rpf shortcut

no rpf shortcut

Parameters

slot/port

Specifies the port that you want to display RPF shortcuts for LSP paths.

Modes

User EXEC mode

Privileged EXEC mode

Usage Guidelines

When RPF lookup results in the LSP path, then another lookup is executed to get the underlying native route and that route's next-hop is used as the RPF.

The no form of the command disables the feature.

Examples

To configure rpf shortcut, use this command in the configuration mode.

device(config)# router pim
device(config-pim-router)# rpf shortcut

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to RPF shortcut for LSP paths information.</td>
</tr>
</tbody>
</table>
rsvp-hello
Configures the RSVP-TE Hello with default values on all the mpls-interfaces, providing the mpls-interface does not have any local-interface level configuration for the same.

Syntax
```
rsvp-hello [ acknowledgments [ interval num | tolerance num ] | interval num | tolerance num ]
no rsvp-hello [ acknowledgments [ interval num | tolerance num ] | interval num | tolerance num ]
```

Parameters
- **acknowledgments**
  Acknowledges RSVP Hellos on the interface supporting RSVP Hello and not having RSVP sessions.
- **interval num**
  Interval between two RSVP Hello requests in seconds. Value range is 1 - 60, default 9.
- **tolerance num**
  Number of unacknowledged RSVP Hello requests, seconds, before a timeout. Value range is 1 - 255, default 3.

Modes
- MPLS configuration mode.
- MPLS interface configuration mode.

Usage Guidelines

**RSVP Hello configuration at the global MPLS RSVP level**

Interval and tolerance for RSVP-TE Hello protocol can be configured at global MPLS RSVP level. The global configuration is pushed to all the mpls-interfaces when the interface level configurations are not present. In addition to these two parameters, one more parameter may be configured at global MPLS RSVP level, namely, acknowledgments.

**Hello-interval and hello-tolerance at mpls-interface level**

RSVP-TE Hello interval and tolerance can be configured at mpls-interface level as well. Interface level configurations take precedence over global configurations. These parameters can be individually configured for each mpls-interface.

By default, acknowledgments are *not sent* on mpls-interface supporting RSVP Hello when no sessions are taking that interface.

Interface-level configuration takes precedence over global configuration.

**CAUTION**

When disabling RSVP hello, disable it on both sides of the link at the same time to avoid bringing down all the RSVP sessions going over that link.

The *no* form of the command does not take interval or tolerance as parameters. Executing the *no rsvp-hello* command on the mpls-interface level sets the RSVP-TE Hello parameters to the globally configured RSVP Hello parameter values. If RSVP
Hello is not configured globally, it disables the RSVP Hello on the mpls-interface. Executing this removes the configuration from the interface level and will no longer display the RSVP Hello configuration at the interface level in the `show configuration` output.

**Examples**

The following example displays the command in the Global configuration mode.

```
device configure terminal
device(config)# router mpls
device(config-mpls)# rsvp
device(config-mpls-rsvp) rsvp-hello
device(config-mpls-rsvp) rsvp-hello interval 15 tolerance 5 acknowledgments
```

The following example displays the command in the Interface configuration mode.

```
device configure terminal
device(config)# router mpls
device(config-mpls-if-e100-1/1)# rsvp
device(config-mpls-if-e100-1/12) rsvp-hello
device(config-mpls-if-e100-1/12) rsvp-hello interval 5 tolerance 2
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
**rsvp-hello acknowledgments**

Configures the RSVP-TE Hello to respond back with Hello ACKs to neighbors not carrying any RSVP sessions.

The `rsvp-hello acknowledgments` command configures the RSVP-TE Hello to respond back with Hello ACKs to neighbors not carrying any RSVP sessions. The configuring for acknowledgments is at the global MPLS RSVP level.

**Syntax**

```plaintext
rsvp-hello acknowledgments
no rsvp-hello acknowledgments
```

**Modes**

MPLS RSVP Hello global configuration mode.

**Usage Guidelines**

By default, RSVP-TE Hello does not send ACKs to neighbors not carrying any RSVP sessions.

The `no` format of this command sets it back to the default behavior of not sending ACKs to neighbors not carrying any RSVP sessions. This erases the configuration line from the global configuration. All the mpls-interfaces supporting RSVP Hello having ZERO sessions to neighbors *do not send HELLO_ACKs for requests sent to those neighbors* (which is the default behavior).

**Examples**

The following example enables RSVP-TE Hello on all mpls-interfaces with default values for hello-interval and hello-tolerance if no interface level specific configuration is present.

```plaintext
device configure terminal
device(config)# router mpls
device(config-mpls)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15
device(config-mpls-rsvp)# rsvp-hello tolerance 5
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**rsvp-hello disable**
Disables RSVP Hello on an mpls-interface.

**Syntax**
```
rsvp-hello disable
no rsvp-hello disable
```

**Modes**
MPLS interface configuration mode.

**Usage Guidelines**
This command erases the configuration line from the configuration like any other `no` command. When there is global configuration, the interface starts picking up globally configured parameters for the RSVP Hello.

If there is no global configuration, the interface does not run RSVP-Hello.

⚠️ **CAUTION**
When disabling RSVP hello, please disable it on both sides of the link at the same time to avoid bringing down all the RSVP sessions going over that link.

The `no` form of the `rsvp-hello` command will not take any parameters other than `disable` at the interface level local configuration. When the parameter needs to be changed to the default value, the user has to execute the normal configuration command.
Examples

The following example displays the command under the Interface configuration.

device (config-mpls-if-e100-1/6)# rsvp-hello disable

The following example displays the RSVP Hello is being disabled on the interface. It generates on the configuration. The RSVP Hello would not be running on this interface irrespective of any global or local configuration present.

device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2

device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgements

device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2

device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/3
device(config-mpls-rsvp)# mpls-interface e1/4

device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 7

device(config-mpls-rsvp)# mpls-interface e1/5

device(config-mpls-rsvp)# mpls-interface e1/6

device(config-mpls-rsvp)# rsvp-hello disable

device(config-mpls-rsvp)# mpls-interface e1/7
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3

The following example displays that the RSVP Hello is configured with the default parameters on the interface. The parameters are auto-generated.

device (config-mpls-if-e100-1/7) rsvp-hello
device (config-mpls-if-e100-1/7) rsvp-hello disable

device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2

device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgements

device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2

device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/3
device(config-mpls-rsvp)# mpls-interface e1/4

device(config-mpls-rsvp)# rsvp-hello interval 20 tolerance 3

device(config-mpls-rsvp)# mpls-interface e1/5
device(config-mpls-rsvp)# mpls-interface e1/6

device(config-mpls-rsvp)# rsvp-hello disable

device(config-mpls-rsvp)# mpls-interface e1/7
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3
device(config-mpls-rsvp)# rsvp-hello disable
The following example displays that the RSVP Hello is enabled back on the interface. The interface starts taking the values that were previously configured on it. When there is no previous interface-specific configuration, then the interface starts taking all of the configuration from the Global level.

When there is no Global configuration as well, then the interface does not run RSVP Hellos.

```
device (config-mpls-if-e100-1/7) no rsvp-hello disable
device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2
device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgments
device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2
device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3
device(config-mpls-rsvp)# mpls-interface e1/3
device(config-mpls-rsvp)# mpls-interface e1/4
device(config-mpls-rsvp)# rsvp-hello interval 20 tolerance 3
device(config-mpls-rsvp)# mpls-interface e1/5
device(config-mpls-rsvp)# mpls-interface e1/6
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 7
device(config-mpls-rsvp)# mpls-interface e1/7
device(config-mpls-rsvp)# mpls-interface e1/8
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3
```

The following example displays that the RSVP Hello’s are being enabled back on the interface.

```
device (config-mpls-if-e100-1/6) no rsvp-hello disable Interval is 15 seconds (Global configuration).
```

```
device configure terminal
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-2
device(config-mpls-policy)# rsvp
device(config-mpls-rsvp)# rsvp-hello interval 15 tolerance 5
device(config-mpls-rsvp)# rsvp-hello acknowledgments
device(config-mpls-rsvp)# mpls-interface e1/1
device(config-mpls-rsvp)# rsvp-hello interval 5 tolerance 2
device(config-mpls-rsvp)# mpls-interface e1/2
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 3
device(config-mpls-rsvp)# mpls-interface e1/3
device(config-mpls-rsvp)# mpls-interface e1/4
device(config-mpls-rsvp)# rsvp-hello interval 20 tolerance 3
device(config-mpls-rsvp)# mpls-interface e1/5
device(config-mpls-rsvp)# mpls-interface e1/6
device(config-mpls-rsvp)# rsvp-hello interval 9 tolerance 7
device(config-mpls-rsvp)# mpls-interface e1/7
device(config-mpls-rsvp)# mpls-interface e1/8
```

NetIron Command Line Interface (CLI) Reference Guide
53-1004199-02 503
## History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sample-recording
Use this command to set the sample recording for the LSP.

Syntax

```plaintext
sample-recording [ enable | disable ]
no sample-recording [ enable | disable ]
```

Command Default
Sample-recording is disabled.

Parameters

- **enable**: Enables sample recording for the LSP.
- **disable**: Disables sample recording for the LSP.

Modes

- MPLS autobw-template configuration mode.
- MPLS LSP mode.

Usage Guidelines

Under the MPLS LSP mode, when autobw-template is configured for this LSP, the sample recording configuration from the template is taken, otherwise sample recording is disabled by default.

This command configures the template to record the sample history.

Under the MPLS autobw-template config mode, the **no** option disables this option.

Examples

The following example shows when the user wants to record the sample history for an LSP or template.

```plaintext
device configure terminal
device(config)# router mpls
device(config-mpls)# autobw-template template1
device(config-mpls-autobw-template-template1)# sample-recording enable

device configure terminal
device(config)# router mpls
device(config-mpls)# lsp lsp1-autobw
device(config-mpls-lsp-lsp1-autobw)# sample-recording enable
```
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**scale-timer**

Configures a scale time factor that increases the timing sensitivity across all configured and default Virtual Router Redundancy Protocol Extended (VRRP-E) timers.

**Syntax**

```
scale-timer vrrp-extended scale-factor
no scale-timer vrrp-extended scale-factor
```

**Command Default**

VRRP timers are not scaled.

**Parameters**

- **vrrp-extended**
  
  A scale time factor can be configured for VRRP-E timers.

- **scale-factor**
  
  A number representing the scale of the division of a VRRP-E configured interval timer or the default interval timer. Valid values are in a range from 1 through 10. The default value is 1.

**Modes**

VRRP-E router configuration mode

**Usage Guidelines**

Configuring the VRRP-E scale timer is supported only in VRRP-E sessions. When a scaling value is configured, the existing timer values are divided by the scaling value. For example: a value of 10 divides the timers by a factor of 10, allowing the default dead interval to be set to 300 ms. Using timer scaling, VRRP-E subsecond convergence is possible if a master VRRP device fails.

**NOTE**

Increased timing sensitivity as a result of this configuration could cause protocol flapping during periods of network congestion.

**NOTE**

Brocade MLX devices only support a scaling factor of 10. For interoperability with MLX devices, use an advertisement interval scale factor of 10.

**Examples**

The following example scales all VRRP-E timers by a factor of 10.

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# scale-timer vrrp-extended 10
```
scale-timer mrp

Decreases the Metro Ring Protocol (MRP) convergence time by changing the MRP scale timer value from 100 ms to 50 ms.

Syntax

    scale-timer mrp
    no scale-timer mrp

Command Default

The default MRP timer value is 50 ms.

Modes

Global configuration mode

Usage Guidelines

The effect of setting the scale timer is that the time taken to move from blocking to preforwarding and preforwarding to forwarding is (preforwarding value - the hello time). This is a significant change to the operation of MRP in the default state which has been described in the previous section.

NOTE
When setting the timer using the command, the actual value used will be exactly half of the input value.

The no form of the command changes the MRP timer tick value to 50 ms.

Examples

The following example decreases the MRP scale timer value from 100 ms to 50 ms.

    device(config)# scale-timer mrp
scp
Copies a license file from an SCP-enabled client to the license database of the device.

Syntax

```
scp license_file_on_hostuser@IP_address: license
```

Command Default

By default, the command is not enabled.

Parameters

- **license_file_on_hostuser@IP_address:**
  Specifies the filename of the license file at the specified IP address.

- **license**
  Specifies the keyword license to be used.

Examples

The following example copies the license file from an SCP-enabled client to the license database.

```
device# scp license.xml terry@10.20.91.39:license
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>07.2.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**set next-hop-tvf-domain**

Configures a TVF domain as the next hop for a route map to support transparent VLAN flooding (TVF) with LAG load balancing.

**Syntax**

```
set next-hop-tvf-domain tvf-domain-ID
no set next-hop-tvf-domain tvf-domain-ID
```

**Command Default**

TVF domain as the route map next hop is not configured.

**Parameters**

`tvf-domain-ID`

Specifies the ID of the TVF domain. Valid values are from 1 through 2016.

**Modes**

Route map configuration mode

**Usage Guidelines**

The `no` form of the command removes the TVF domain as the route map next hop.

**Examples**

The following example configures a TVF domain 1 as the next hop for the test-route route map.

```
device(config)# route-map test-route permit 99
device(config-routemap test-route)# set next-hop-tvf-domain 1
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sflow nullO-sampling

Enables the nullO sampling.

Syntax

sflow nullO-sampling slot/port  
nosflow nullO-sampling slot/port

Parameters

slot port

Enables nullO sampling for a specific slot and port.

Modes

Global configuration mode

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to display sFlow nullO sampling status.</td>
</tr>
</tbody>
</table>
shortcuts isis
Files ISIS IGP protocol not to use the configured LSP metric values for the shortcuts when doing SPF calculations.

Syntax

```
shortcuts isis { level1 | level2 } [ announce announce-metric value | ignore-lsp-metric ] [ announce [ announce-metric value ] ]
[ relative-metric +/- value ]
```

```
no shortcuts isis { level1 | level2 } [ announce announce-metric value | ignore-lsp-metric ] [ announce [ announce-metric value ] ] [ relative-metric +/- value ]
```

Command Default

The configured LSP metric is used as the shortcut's cost when performing IGP SPF calculation.

Parameters

- **level1**
  - A level1 router routes traffic only within the area that includes the router. To forward traffic to another area, a level1 router sends the traffic to the nearest level2 router.

- **level2**
  - A level2 router routes traffic between areas within a domain.

- **announce**
  - Announces tunnel into ISIS domain.

  - **announce-metric value**
    - Announces the metric value between 1-16777215. The default is 10.

- **ignore-lsp-metric**
  - Ignore configured LSP metric as the shortcut's cost when performing IGP SPF calculation.

  - **announce**
    - Announce tunnel into ISIS domain.

  - **announce-metric value**
    - Announces the metric value between 1-16777215. The default is 10.

- **relative-metric**
  - Configures relative metric.

  - **+/- value**
    - The + or – sign is required. + denotes a positive number. – denotes a negative number. For value, enter a value from 1 - 16777215. The default is 0 (zero).

Modes

MPLS LSP sub configuration mode (config-mpls-lsp-lspxxx).
Usage Guidelines

Use the **no** form of this command without other optional keywords to disable this feature. The LSP must be disabled before configuring/de-configuring this feature.

When “ignore-lsp-metric” is enabled, ISIS will behave like the shortcut LSP metrics are not configured.

When announce is not enabled and a metric is not explicitly configured under the LSP configuration mode of the CLI, the relative metric is used to compute the shortcut cost.

Examples

The following example displays that when the tunnel is enabled, the user must disable it before enabling announce, then re-enable the tunnel.

```plaintext
device(config-mpls-lsp-tomu3)# disable
Disconnecting signaled LSP tomu3
device(config-mpls-lsp-tomu3)# shortcuts isis level2 announce
device(config-mpls-lsp-tomu3)# enable
Connecting signaled LSP tomu3
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.0</td>
<td>This command is modified to include the new option keyword <strong>ignore-lsp-metric</strong>. This is added to the existing shortcut command under the LSP configuration mode.</td>
</tr>
</tbody>
</table>
**shortcuts ospf**

Enables OSPF shortcuts over an LSP tunnel to forward traffic to destinations within an OSPF routing domain through an LSP tunnel.

**Syntax**

```plaintext
shortcuts ospf [ ignore-lsp-metric ]
no shortcuts ospf [ ignore-lsp-metric ]
```

**Command Default**

OSPF shortcuts over an LSP tunnel is not enabled.

**Parameters**

- `ignore-lsp-metric`
  
  Forces OSPF to ignore the configured LSP metric values as the shortcut cost when performing SFP calculations. The effective metric of the shortcut is derived by summing up all the path’s cost spanned by the shortcut.

**Modes**

MPLS LSP mode.

**Usage Guidelines**

The LSPs must originate and terminate within the same OSPF area. When OSPF shortcuts over an LSP tunnel is enabled, OSPF directs routes that are reachable from the egress router of a shortcut-enabled LSP to an LSP tunnel as the outgoing interface.

The **no** form of this command without an option disables OSPF shortcuts over an LSP tunnel.

The **no** form of this command with the `ignore-lsp-metric` option disables the forcing of OSPF to ignore the configured LSP metric values as the shortcut cost when performing SFP calculations.

**Examples**

The following example is a configuration of the tunnel1 LSP to specify the egress router with a router ID of 10.2.2.2 and enable it for OSPF shortcuts.

```plaintext
device# configure terminal
device(config)# router mpls
device(config-mpls)# lsp tunnel1
device(config-mpls-lsp)# to 10.2.2.2
device(config-mpls-lsp)# shortcuts ospf
device(config-mpls-lsp)# enable
```
short-path-forwarding

Enables short-path forwarding on a Virtual Router Redundancy Protocol (VRRP) router.

Syntax

```
short-path-forwarding [ revert-priority number ]
no short-path-forwarding [ revert-priority number ]
```

Command Default

Short-path forwarding is disabled.

Parameters

`revert-priority number`

Allows additional control over short-path forwarding on a backup router. If you configure this option, the revert-priority number acts as a threshold for the current priority of the session, and only if the current priority is higher than the revert-priority will the backup router be able to route frames. The range of revert-priority is 1 to 254.

Modes

VRRP-E router configuration mode

Usage Guidelines

Short-path forwarding means that a backup physical router in a virtual router attempts to bypass the VRRP-E master router and directly forward packets through interfaces on the backup router.

This command can be used for VRRP-E, but not for VRRP. You can perform this configuration on a virtual Ethernet (VE) interface only.

Enter the `no short-path-forwarding` command to remove this configuration.

Examples

To enable short-path forwarding for a VRRP-E instance:

```
device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# slow-start 40
device(config-vrrpe-router)# short-path-forwarding
```
Show Commands

**show access-list accounting**
Displays Access Control List (ACL) accounting statistics of IPv4 ACLs, IPv6 ACLs, and Layer 2 ACLs.

show access-list accounting brief [ rate-limit | [ l2 | uda ] [ policy-based-routing [ omit-zero ] ]]
show access-list accounting ethernet slot/port { in | out } [ rate-limit | [ l2 | uda ] [ policy-based-routing [ omit-zero ] ]]
show access-list accounting ve ve-number { in | out } [ rate-limit | [ l2 | uda ] [ policy-based-routing [ omit-zero ] ]]

**brief**
Displays the ACL accounting summary.

**rate-limit**
Displays rate-limit accounting information.

**l2**
Displays Layer 2 ACL accounting information.

**uda**
Displays UDA ACL accounting information.

**policy-based-routing**
Displays policy-based routing accounting information.

**omit-zero**
Specifies not to display ACL entry with 0 packet/bits.

**in**
Displays statistics of the inbound packets.

**out**
Displays statistics of the outbound packets.

**ethernet slot/port**
Displays the accounting statistics for ACLs on a physical interface.

**ve ve-number**
Displays the statistics for ACLs bound to ports that are members of a virtual routing interface.

User EXEC mode

The output displays information about IPv4 ACLs, IPv6 ACLs, or Layer 2 ACLs, based on the configuration of the port or interface. The clear command can be used clear the PBR statistics on the specified interface.

The **show access-list accounting** command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Identifies the interface.</td>
</tr>
<tr>
<td>In ACL</td>
<td>Displays the name of the ingress ACL.</td>
</tr>
<tr>
<td>Total In Hit</td>
<td>Displays the number of ingress-packet hits during the specified interval:</td>
</tr>
</tbody>
</table>
### Output field Description

- 1s—one second
- 1m—one minute
- 5m—five minutes
- acc—total accumulated packet hits

**Out ACL**
Displays the name of the egress ACL.

**Total Out Hit**
Displays the number of egress-packet hits during the specified interval.

The following example displays the incoming accounting information on a physical interface.

```
device(config)# enable-acl-counter
device# show access-list accounting ethernet 1/1 in
Inbound:
ACL 1
0: permit host 29.7.51.11
   Hit count: (1 sec)                    0   (1 min)                    0
   (5 min)                    0   (accum)                    0
1: permit host 29.7.51.9
   Hit count: (1 sec)                    0   (1 min)                    0
   (5 min)                    0   (accum)                    0
2: permit host 29.7.51.10
   Hit count: (1 sec)                    0   (1 min)                    0
   (5 min)                    0   (accum)                    0
3: permit host 29.7.51.14
   Hit count: (1 sec)                    0   (1 min)                    0
   (5 min)                    0   (accum)                    0
4: permit host 29.7.51.15
   Hit count: (1 sec)                    0   (1 min)                    0
   (5 min)                    0   (accum)                    0
```

The following example displays the Layer 2 PBR incoming accounting information on a physical interface.

```
device(config)# show access-list accounting ethernet 1/2 in l2 policy-based-routing
L2 Policy based Routing Accounting Information:
Routemap l2pbr10
ACL x10
0:   10:  permit any any any etype any
     Hit count: (1 sec)                    0  (1 min)                    0
     (5 min)                    0  (accum)                    0
```

The following example displays the general brief accounting summary.

```
device# show access-list accounting brief
Int    In ACL              Total In Hit   Out ACL             Total Out Hit
1/1         1                     0(1s)         2                     0(1s)
            0(1m)                               0(1m)
            0(5m)                               0(5m)
            0(ac)                               0(ac)
```

The following example displays the Layer 2 PBR accounting summary.

```
device# show access-list accounting brief l2 policy-based-routing
Int    In ACL              Total In Hit   Out ACL             Total Out Hit
1/1         x10                     0(1s)         0                     0(1s)
            0(1m)                               0(1m)
            0(5m)                               0(5m)
            0(ac)                               0(ac)
4/2                            x10                     0(1s)         0                     0(1s)
            0(1m)                               0(1m)
            0(5m)                               0(5m)
            0(ac)                               0(ac)
```

---

Show Commands

NetIron Command Line Interface (CLI) Reference Guide
53-1004199-02
The following example displays the UDA PBR statistics on the specified interface.

```plaintext
device(config)# show access-list accounting ethernet 3/1 in uda policy-based-routing
Policy based Routing Accounting Information:
Routemap route1
Acl ACLNameTest112345679-023456789-0123456789
  0: sequence 10 permit 100 any any 1234 ffff any
    Hit count: (1 sec) 0 (1 min) 0
    (5 min) 0 (accum) 0
    0(ac)
```

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00b</td>
<td>The <code>l2</code> option was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>The command was modified to display the UDA PBR statistics on the specified interface.</td>
</tr>
</tbody>
</table>
show access-list bindings

Displays all access-lists bound to different interfaces. This includes both rule-based ACL and receive access-control list (rACL) information.

Syntax

show access-list bindings

Modes

User EXEC node

Examples

The following example displays all access-list bindings.

Brocade(config)# show access-list bindings
L4 configuration:
! interface ethe 2/1
  mac access-group SampleACL in
  !
show access-list receive accounting

Displays accounting information for a receive access-control list (rACL) or brief information for all rACLs.

Syntax

```
show access-list receive accounting { acl-num | name acl-name | brief }
```

Parameters

- **acl-num**
  Specifies a receive ACL in number format. Valid values are 1 through 99 for standard ACLs and 100 through 199 for extended ACLs.

- **name acl-name**
  Specifies a receive ACL in name format.

- **brief**
  Displays receive-ACL accounting in brief.

Modes

User EXEC mode

Examples

The following example displays rACL accounting information for an ACL named "acl_ext1".

```
device(config)# show access-list receive accounting name acl_ext1
IP Receive ACL Accounting Information:
  IP Receive ACL acl_ext1
  ACL hit count for software processing (accum)                       0
  HW counters:
    0: permit tcp any host 10.10.10.14
      Hit count: (1 sec) 0 (1 min) 0 (5 min) 0 (accum) 0
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was modified to support named ACLs, in addition to numbered ACLs.</td>
</tr>
</tbody>
</table>
show acl-policy

Displays the ACL policy configuration.

Syntax

show acl-policy

Modes

Privileged EXEC mode

Examples

The following example displays the ACL policy configuration.

device# show acl-policy
ACL-Policy configuration:
! display-config-format
accounting-no-sort
force-delete-bound-acl
suppress-acl-seq
display-def-acl-seq
acl-skip-boot-checks
acl-conflict-check
acl-duplication-check
display-pkt-bit-rate
enable-acl-cam-sharing
acl-frag-conservative
enable-acl-counter
statistics-load-interval 60
suppress-ipv6-priority-mapping
disable-acl-for-gre
disable-acl-for-6to4
!

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show arp

Displays an IP mechanism that the routers use to learn the Media Access Control (MAC) address of a device on the network.

Syntax

```
show arp [ ip-addr [ ip-mask ] | num-entries-to-skip | ethernet slot / port | mac-address xxxxxxx.xxxx [ MAC-mask ] | vrf vrf-name ]
```

Parameters

- `ip_addr` Specifies IP address.
- `ip_mask` Specifies IP subnet.
- `num-entries-to-skip` Number of entries to skip.
- `ethernet slot/port` Displays specified ethernet port.
- `mac-address xxxxxxx.xxxx` Displays the mac address of the specified entry.
- `MAC-mask` Specifies a mask for display of multiple MAC addresses.
- `vrf vrf_name` Displays ARP entries belonging to a given VRF instance.

Modes

User EXEC mode

Usage Guidelines

show arp

This command operates in all modes.

Command Output

The `show arp` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the entry.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the entry.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of entry. The options are:</td>
</tr>
</tbody>
</table>
Output field | Description
---|---
| • Static: The Layer 3 switch loaded the entry from the static ARP table when the device for the entry was connected to the Layer 3 switch.
| • Dynamic: The Layer 3 switch learned the entry from an incoming packet.
| • DHCP - The Layer 3 Switch learned the entry from the DHCP binding address table. In this case, the port number is not available until the entry gets resolved through ARP.

Age | The number of minutes before which the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.

Port/Port | The ‘To’ and ‘From’ ports. If the ARP entry type is DHCP, the port number is not available until the entry gets resolved through ARP.

Vpls-Id:Vlan | Displays VPLS identification information.

Vpls-Id:Peer | Displays VPLS peer information.

Examples

The following example displays the `show arp` command output:

device(config)# show arp
Total number of ARP entries: 4
Entries in default routing instance:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Age</th>
<th>Port/Port</th>
<th>(Vpls-Id:Vlan)/(Vpls-Id:Peer)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.25.104.1</td>
<td>0000.0012.3eb5</td>
<td>Static</td>
<td>None</td>
<td>4/1</td>
<td>(101, 26)</td>
</tr>
<tr>
<td>10.25.104.3</td>
<td>0000.000f.c200</td>
<td>Dynamic</td>
<td>0</td>
<td>mgmt1</td>
<td></td>
</tr>
<tr>
<td>10.1.1.2</td>
<td>0000.00f8.0090</td>
<td>Dynamic</td>
<td>1</td>
<td>mgmt1</td>
<td></td>
</tr>
<tr>
<td>10.25.104.1</td>
<td>0000.0012.3eb5</td>
<td>Static</td>
<td>None</td>
<td></td>
<td>(21, 10.32.332.1)</td>
</tr>
</tbody>
</table>
show arp-guard-access-list

Displays details for a specified ARP-guard access list (ACL) or all ARP-guard ACLs.

Syntax

show arp-guard-access-list { all | name arp-guard-access-list }

Parameters

all

Specifies all ARP-guard ACLs.

name arp-guard-access-list

Specifies the name of an ARP-guard access list.

Modes

User EXEC mode
Examples

The following example displays information about the ARP guard access list named C5-global-arp.

device# show arp-guard-access-list name C5-global-arp
Arp-Guard : C5-global-arp
Number of rules :  6
Number of Ports : 16
Rules configured
permit  40  31.0.8.1  0012.f290.7400
permit  1500 31.0.10.2  0000.0015.0000
permit  1001 100.0.0.2  0024.38a3.6e00
permit  20 41.0.100.1  0024.38a3.6e00
permit  80 51.0.4.2  748e.f874.4900
permit any 31.0.11.1  0012.f290.7400

The following example displays information about all the ARP guard access list.

device# show arp-guard-access-list all
Arp-guard configuration:
!
arp-guard-access-list C5-8
!
arp-guard-access-list MCT-A3
permit any 31.0.10.2 0000.0300.0000
permit any 31.0.10.3 0000.0300.0001
permit any 31.0.10.4 0000.0300.0002
permit any 31.0.10.5 0000.0300.0003
permit any 31.0.11.1 any
permit any 31.0.11.2 any
permit any 31.0.11.3 any
!
arp-guard-access-list C5-global-arp
permit 40  31.0.8.1  0012.f290.7400
permit 1500 31.0.10.2  0000.0015.0000
permit 1001 100.0.0.2  0024.38a3.6e00
permit 20 41.0.100.1  0024.38a3.6e00
permit 80 51.0.4.2  748e.f874.4900
permit any 31.0.11.1  0012.f290.7400
!
arp-guard-access-list AS201
permit any 1.1.1.1 any
permit any 1.1.1.1 0001.0001.0001
!

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROS.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show arp-guard port-bindings
Displays list of ports associated with an ARP-guard access-list (ACL) or with all ARP-guard ACLs.

Syntax
```bash
show arp-guard port-bindings { arp-guard-access-list | all }
```

Parameters
- `arp-guard-access-list` Displays port-binding associations for an ARP-guard access list.
- `all` Displays port-binding associations for all ARP-guard ACLs.

Modes
User EXEC mode

Usage Guidelines
This command can be entered in most configuration modes. See the Examples section for several examples in different configuration modes.

Command Output
The `show arp-guard port-bindings` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arp-Guard</td>
<td>Displays the name of the ARP-guard.</td>
</tr>
<tr>
<td>Number of Ports</td>
<td>Displays the total number of ports associated with this ARP-guard.</td>
</tr>
<tr>
<td>Port Lists</td>
<td>Displays the list of ports associated with that ARP-guard.</td>
</tr>
</tbody>
</table>

Examples
The following example displays information about the ARP-guard port bindings for AS200.

```bash
device(config-if-e10000-1/8)# show arp-guard port-bindings AS200
Arp-Guard : AS200
Number of Ports : 1
Port Lists : ethe 1/8
```
The following example displays information about the ports associated with ARP-guard.

```
device# show arp-guard port-bindings all
Arp-Guard Port Bindings:
Arp-Guard        : ag1
 Number of Ports : 0

Arp-Guard        : ag2
 Number of Ports : 2
 Ethe 1/2        Log : Disabled
 Ethe 1/4        Log : Disabled

Arp-Guard        : ag3
 Number of Ports : 8
 Ethe 1/1        Log : Disabled
 Ethe 2/1        Log : Enabled   Num of violations : Default
 Ethe 2/2        Log : Enabled   Num of violations : 32
 Ethe 2/3        Log : Enabled   Num of violations : 32
 Ethe 2/4        Log : Enabled   Num of violations : 32
 Ethe 2/6        Log : Disabled
 Ethe 3/1        Log : Enabled   Num of violations : Default
 Ethe 4/1        Log : Enabled   Num of violations : Default
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show arp-guard statistics ethernet
Displays ARP-guard statistical information.

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

Parameters
- **all**
  Displays all ARP-guard port statistics.
- **slot/port**
  Displays statistics specific to a port.
- **vlan vlan-id**
  Displays statistics specific to a VLAN on a port. The VLAN ID range is from 1 through 4090.

Modes
User EXEC mode

Usage Guidelines
This command displays statistics for LAG primary ports, but not for secondary ports.

Command Output
The `show arp-guard statistics ethernet` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>Vlan-id</td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>Total_Arp_pkts_captured</td>
<td>The total number of ARP packets captured.</td>
</tr>
<tr>
<td>Total_Arp_pkts_forwarded</td>
<td>The total number of ARP packets forwarded</td>
</tr>
<tr>
<td>Total_Arp_pkts_dropped</td>
<td>The total number of ARP packets dropped</td>
</tr>
<tr>
<td>LAG : Prim</td>
<td>Displayed only in the show arp-guard statistics ethernet all alone. To denote LAG ID and its Primary port for that LAG associated with all the ARP-guard enabled ports.</td>
</tr>
</tbody>
</table>
Examples

The following example displays statistics information for all the ports.

device(config)# show arp-guard statistics ethernet all

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan-id</th>
<th>Total_Arp_pkts_captured</th>
<th>Total_Arp_pkts_forwarded</th>
<th>Total_Arp_pkts_dropped</th>
<th>LAG : Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prim 1/1 (Def/Untag) 1</td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>1</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>2</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2/1 (Def/Untag) 1</td>
<td>3</td>
<td>10000</td>
<td>9000</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>2</td>
<td>10000</td>
<td>9000</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>4</td>
<td>10000</td>
<td>9000</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>5</td>
<td>10000</td>
<td>9000</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

The following example displays statistics information for any individual port.

device(config)# show arp-guard statistics ethernet 1/1

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan-id</th>
<th>Total_Arp_pkts_captured</th>
<th>Total_Arp_pkts_forwarded</th>
<th>Total_Arp_pkts_dropped</th>
<th>LAG : Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prim 1/1 (Def/Untag) 1</td>
<td>3</td>
<td>10000</td>
<td>9000</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>2</td>
<td>10000</td>
<td>9000</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

The following example displays statistics information for a VLAN of the ARP-guard-enabled port.

device# show arp-guard statistics ethernet 1/1 vlan 2

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan-id</th>
<th>Total_Arp_pkts_captured</th>
<th>Total_Arp_pkts_forwarded</th>
<th>Total_Arp_pkts_dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>2</td>
<td>10000</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>R05.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show bfd

Displays Bidirectional Forwarding Detection (BFD) information.

Syntax

show bfd

Modes

User EXEC mode

Command Output

The show bfd command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD State</td>
<td>Specifies whether BFD is enabled or disabled on the device.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version of the BFD protocol operating on the device.</td>
</tr>
<tr>
<td>Use PBIF Assist</td>
<td>Specifies the status of PCI Bus Interface (PBIF) Assist.</td>
</tr>
<tr>
<td>Current Registered Protocols</td>
<td>Specifies which protocols are registered to use BFD on the device. Possible values are mpls/0, ospf/0, ospf6/0, or isis_task/0.</td>
</tr>
<tr>
<td>All Sessions</td>
<td></td>
</tr>
<tr>
<td>Current:</td>
<td>The number of BFD sessions currently operating on the device.</td>
</tr>
<tr>
<td>Maximum Allowed</td>
<td>The maximum number of BFD sessions that are allowed on the device. The maximum number of sessions supported is 250 for Brocade NetIron MLX Series devices and Brocade NetIron XMR Series devices and 40 for Brocade NetIron CES Series devices.</td>
</tr>
<tr>
<td>Maximum Exceeded Count</td>
<td>The number of times the request to set up a BFD session was declined because it would have resulted in exceeding the maximum number of BFD sessions allowed on the device.</td>
</tr>
<tr>
<td>LP Sessions:</td>
<td></td>
</tr>
<tr>
<td>Maximum Allowed on LP</td>
<td>The maximum number of BFD sessions that are allowed on an interface module. The maximum number of sessions supported on an interface module is 40 for Brocade NetIron XMR Series devices and Brocade NetIron MLX Series devices, and 20 for Brocade NetIron CES Series devices.</td>
</tr>
<tr>
<td>Maximum Exceeded Count for LPs</td>
<td>The number of times the request to set up a BFD session was declined because it would have resulted in exceeding the maximum number of BFD sessions allowed on an interface module.</td>
</tr>
<tr>
<td>LP</td>
<td>The number of the interface module for which the Current Session Count is displayed.</td>
</tr>
<tr>
<td>TX/RX Sessions</td>
<td>The number of Transmit (Tx) and Receive (Rx) BFD sessions currently operating on the specified interface module.</td>
</tr>
<tr>
<td>BFD Enabled ports count</td>
<td>The number of ports on the device that have been enabled for BFD.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that BFD is enabled on.</td>
</tr>
<tr>
<td>MinTx</td>
<td>The interval in milliseconds between which the device desires to send a BFD message from this port to its peer.</td>
</tr>
<tr>
<td>MinRx</td>
<td>The interval in milliseconds that this device desires to receive a BFD message from its peer on this port.</td>
</tr>
<tr>
<td>Mult</td>
<td>The number of times that the device will wait for the MinRx time on this port before it determines that its peer device is non-operational.</td>
</tr>
<tr>
<td>Sessions</td>
<td>The number of BFD sessions originating on this port.</td>
</tr>
</tbody>
</table>
Examples

The following example displays BFD information for the device.

device# show bfd

BFD State: ENABLED Version: 1 Use PBIF Assist: Y
Current Registered Protocols: ospf/0  ospf6/0
All Sessions: Current: 4 Maximum Allowed: 100 Maximum Exceeded Count: 0
LP Sessions: Maximum Allowed on LP: 40 Maximum Exceeded Count for LPs: 0
LP Tx/Rx Sessions
1 4/4 2 2/2 3 0/0 4 0/0
5 0/0 6 0/0 7 0/0 8 0/0
9 0/0 10 0/0 11 0/0 12 0/0
13 0/0 14 0/0 15 0/0 16 0/0
BFD Enabled ports count: 2
Port MinTx MinRx Mult Sessions
eth 2/1 100 100 3 2
eth 3/1 100 100 3 2

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was modified to include MPLS in the registered protocol list. In addition, the number of sessions on the LP is shown separately as TX and RX.</td>
</tr>
</tbody>
</table>
**show bfd applications**

Displays Bidirectional Forwarding Detection (BFD) registered protocol information.

**Syntax**

```
show bfd applications
```

**Modes**

User EXEC mode

**Command Output**

The `show bfd applications` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Protocols Count</td>
<td>Total number of protocols registered to use BFD on the device.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Which protocols are registered to use BFD on the device.</td>
</tr>
<tr>
<td>VRFID</td>
<td>The VRFID of the protocol.</td>
</tr>
<tr>
<td>Parameter</td>
<td>The parameter value passed by the protocol during registration with BFD.</td>
</tr>
<tr>
<td>HoldoverInterval</td>
<td>The time by which the BFD session down notification is delayed. If within that holdover time, the BFD session is up, then it is not notified of the BFD session flap.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays BFD registered protocol information for the device.

```
device# show bfd applications
Registered Protocols Count: 3
Protocol  VRFID  Parameter  HoldoverInterval
isis      0      0         2
ospf6     0      1         10
ospf      0      0         5
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>The command was modified to include MPLS information.</td>
</tr>
</tbody>
</table>
show bfd mpls
Displays information about MPLS Bi-Directional Forwarding (BFD) sessions. You can filter BFD sessions based on LSP name or egress RSVP session ID.

Syntax

```
show bfd mpls
show bfd mpls detail
show bfd mpls lsp lsp-name
show bfd mpls rsvp-session src_addr dest-addr tunnel-id
```

Parameters

detail
Displays the MPLS BFD session in detail.

lsp lsp-name
Displays the MPLS BFD session associated with a specific LSP.

rsvp-session src_addr dest-addr tunnel-id
Displays the MPLS BFD session associated with the egress RSVP session specified using the source address, destination address, and tunnel ID options.

Modes
User EXEC mode

Usage Guidelines
If no optional keywords are entered, information about all MPLS BFD sessions is displayed. You can filter BFD session based on LSP name or egress RSVP session ID or show detailed MPLS BFD information. For MPLS BFD sessions associated with LSP, the LSP name is displayed. For a BFD session associated with an egress RSVP session, the RSVP session ID issued to identify the BFD session is displayed.

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show bfd neighbors

Displays detailed Bidirectional Forwarding Detection (BFD) neighbor information.

Syntax

```
show bfd neighbors [ ip-address | ipv6-address ]
```

Parameters

- **ip-address**
  Specifies the IP address of a neighbor.

- **ipv6-address**
  Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Command Output

The `show bfd neighbors` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of Neighbor entries</td>
<td>The number of neighbors that have established BFD sessions with ports on this device.</td>
</tr>
<tr>
<td>NeighborAddress</td>
<td>The IPv4 or IPv6 address of the remote peer.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the BFD session:</td>
</tr>
<tr>
<td></td>
<td>• UP</td>
</tr>
<tr>
<td></td>
<td>• DOWN</td>
</tr>
<tr>
<td></td>
<td>• A.DOWN - The administrative down state.</td>
</tr>
<tr>
<td></td>
<td>• INIT - The initialization state.</td>
</tr>
<tr>
<td></td>
<td>• UNKNOWN - The current state is unknown.</td>
</tr>
<tr>
<td>Interface</td>
<td>The logical port (physical or virtual port) on which the peer is known.</td>
</tr>
<tr>
<td>Holddown</td>
<td>The interval in milliseconds after which the session will transition to the down state if no message is received.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in milliseconds at which the local device sends BFD messages to the remote peer.</td>
</tr>
<tr>
<td>R/H</td>
<td>R - Heard from Remote. Displays Y for Yes or N for No.</td>
</tr>
<tr>
<td></td>
<td>H - Hops. Display S for single hop or M for multihop.</td>
</tr>
</tbody>
</table>

Examples

The following example displays BFD neighbor information for the device.

```
device# show bfd neighbors
Total number of Neighbor entries: 2
NeighborAddress  State  Interface  Holddown  Interval  R/H
10.14.1.1        UP     eth 3/1   300000    100000    Y/S
10.2.1.1          UP     eth 2/1   300000    100000    Y/S
```
show bfd neighbors bgp

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for BGP.

Syntax

```
show bfd neighbors bgp [ details ] [ ip-address | ipv6-address ]
```

Parameters

details

Displays detailed neighbor interface information.

ip-address

Specifies the IP address of a neighbor.

ipv6-address

Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Command Output

The `show bfd neighbors bgp details` command displays the following information:

<table>
<thead>
<tr>
<th>Output Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Entries</td>
<td>Total number of BFD sessions.</td>
</tr>
<tr>
<td>NeighborAddress</td>
<td>IPv4 or IPv6 address of the remote peer.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the BFD session:</td>
</tr>
<tr>
<td></td>
<td>• UP</td>
</tr>
<tr>
<td></td>
<td>• DOWN</td>
</tr>
<tr>
<td></td>
<td>• A.DOWN - The administrative down state.</td>
</tr>
<tr>
<td></td>
<td>• INIT - The initialization state.</td>
</tr>
<tr>
<td></td>
<td>• UNKNOWN - The current state is unknown.</td>
</tr>
<tr>
<td>Interface</td>
<td>The logical port on which the peer is known.</td>
</tr>
<tr>
<td>Holddown</td>
<td>The interval in milliseconds after which the session will transition to the down state if no message is received.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in milliseconds at which the local device sends BFD messages to the remote peer.</td>
</tr>
<tr>
<td>R/H</td>
<td>R - Heard from Remote. Displays Y for Yes or N for No.</td>
</tr>
<tr>
<td></td>
<td>H - Hops. Display S for single hop or M for multihop.</td>
</tr>
<tr>
<td>Registered Protocols</td>
<td>Specifies which protocols are registered to use BFD on this port.</td>
</tr>
<tr>
<td>Local</td>
<td>The local device</td>
</tr>
<tr>
<td>Disc</td>
<td>Value of the local discriminator field in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Diag</td>
<td>Value of the diagnostic field in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>Demand</td>
<td>Value of the demand bit in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>Poll</td>
<td>Value of the poll bit in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>MinTxInterval</td>
<td>The interval in milliseconds during which the device will send a BFD message from this local neighbor port to the peer.</td>
</tr>
<tr>
<td>MinRxInterval</td>
<td>The interval in milliseconds that the neighbor device waits to receive a BFD message from the peer on this local port.</td>
</tr>
<tr>
<td>Multiplier</td>
<td>The number of times the neighbor device will wait for the MinRxInterval time on this port before it determines the peer device is non-operational.</td>
</tr>
<tr>
<td>Remote:</td>
<td>Remote peer.</td>
</tr>
<tr>
<td>Disc</td>
<td>Value of the local discriminator field in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>Diag</td>
<td>Value of the diagnostic field in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>Demand</td>
<td>Value of the demand bit in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>Poll</td>
<td>Value of the poll bit in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>MinTxInterval</td>
<td>The interval in milliseconds during which the device will send a BFD message from the remote neighbor port to the peer.</td>
</tr>
<tr>
<td>MinRxInterval</td>
<td>The interval in milliseconds that the neighbor device waits to receive a BFD message from the peer on this remote port.</td>
</tr>
<tr>
<td>Multiplier</td>
<td>The number of times that the remote neighbor device will wait for the MinRxInterval time on this port before it determines that the peer device is non-operational.</td>
</tr>
<tr>
<td>Stats:</td>
<td>Statistics</td>
</tr>
<tr>
<td>Rx</td>
<td>Total number of BFD control messages received from the remote peer.</td>
</tr>
<tr>
<td>Tx</td>
<td>Total number of BFD control messages sent to the remote peer.</td>
</tr>
<tr>
<td>SessionUpCount</td>
<td>The number of times the session has transitioned to the up state.</td>
</tr>
<tr>
<td>SysUpTime</td>
<td>The amount of time that the system has been up.</td>
</tr>
<tr>
<td>Session Uptime</td>
<td>The amount of time the session has been in the up state.</td>
</tr>
<tr>
<td>LastSessionDownTimestamp</td>
<td>The system time at which the session last transitioned from the up state to some other state.</td>
</tr>
<tr>
<td>Physical Port</td>
<td>The physical port on which the peer is known.</td>
</tr>
<tr>
<td>Vlan Id</td>
<td>The VLAN ID of the VLAN on which the physical port is resident.</td>
</tr>
</tbody>
</table>
Examples

The following example displays BFD neighbor information for BGP for the device.

```
device# show bfd neighbors bgp
```

Neighbor AS4 Capability Negotiation:
As-path attribute count: 2
Outbound Policy Group:
ID: 1, Use Count: 3
BFD:Enabled,BFDSessionState:UP,Multihop:Yes
LastBGP-BFDEvent:RX:Up,BGP-BFDError:No Error
NegotiatedTime(msec):Tx:1000000,Rx:1000000,BFDHoldTime:3000000
HoldOverTime(sec) Configured:22,Current:0,DownCount:0
TCP Connection state: ESTABLISHED, flags:00000044 (0,0)
Maximum segment size: 1460

The following example displays detailed BFD neighbor information for BGP for a Brocade NetIron MLX Series or Brocade Netiron XMR Series device.

```
device# show bfd neighbors bgp details
```

<table>
<thead>
<tr>
<th>NeighborAddress</th>
<th>State</th>
<th>Interface</th>
<th>Holddown</th>
<th>Interval</th>
<th>R/H</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.101.101.100</td>
<td>UP</td>
<td>ve 3</td>
<td>3000000</td>
<td>1000000</td>
<td>Y/M</td>
</tr>
</tbody>
</table>
| Local: Disc: 7, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
| Remote: Disc: 8, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3 |
| Stats: RX: 14682 TX: 12364 SessionUpCount: 1 at SysUpTime: 0:1:37:50.600, LastSessionDownTimestamp: 0:0:0:0.0 |
| Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3 |

<table>
<thead>
<tr>
<th>NeighborAddress</th>
<th>State</th>
<th>Interface</th>
<th>Holddown</th>
<th>Interval</th>
<th>R/H</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.100.100.100</td>
<td>UP</td>
<td>ve 3</td>
<td>3000000</td>
<td>1000000</td>
<td>Y/M</td>
</tr>
</tbody>
</table>
| Local: Disc: 7, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
| Remote: Disc: 8, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3 |
| Stats: RX: 14232 TX: 12046 SessionUpCount: 1 at SysUpTime: 0:1:37:49.650, LastSessionDownTimestamp: 0:0:0:0.0 |
| Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3 |

<table>
<thead>
<tr>
<th>NeighborAddress</th>
<th>State</th>
<th>Interface</th>
<th>Holddown</th>
<th>Interval</th>
<th>R/H</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.1</td>
<td>UP</td>
<td>ve 3</td>
<td>3000000</td>
<td>1000000</td>
<td>Y/M</td>
</tr>
</tbody>
</table>
| Local: Disc: 7, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
| Remote: Disc: 8, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3 |
| Stats: RX: 15652 TX: 12044 SessionUpCount: 1 at SysUpTime: 0:1:37:48.725, LastSessionDownTimestamp: 0:0:0:0.0 |
| Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3 |

<table>
<thead>
<tr>
<th>NeighborAddress</th>
<th>State</th>
<th>Interface</th>
<th>Holddown</th>
<th>Interval</th>
<th>R/H</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.102.102.100</td>
<td>UP</td>
<td>ve 3</td>
<td>3000000</td>
<td>1000000</td>
<td>Y/M</td>
</tr>
</tbody>
</table>
| Local: Disc: 7, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3
| Remote: Disc: 8, Diag: 0, Demand: 0 Poll: 0, MinTxInterval: 1000000, MinRxInterval: 1000000, Multiplier: 3 |
| Stats: RX: 14232 TX: 12044 SessionUpCount: 1 at SysUpTime: 0:1:37:48.550, LastSessionDownTimestamp: 0:0:0:0.0 |
| Physical Port:TX: eth 1/1,RX: eth 1/1,Vlan Id: 3 |
The following example displays detailed BFD neighbor information for BGP for a Brocade Netiron CES Series or Brocade Netiron CER Series device.

device# show bfd neighbors bgp details

Total Entries: 1  R:RXRemote (Y:Yes/N:No) H:Hop (S:Single/M:Multi)
NeighborAddress    State   Interface   Holddown Interval R/H
fe80::224:38ff:fe79:9310       UP       eth 1/17  1500000    500000   Y/S

Registered Protocols (Protocol/VRFID): bgp/0
Local: Disc: 8, Diag: 0, Demand: 0 Poll: 0
    MinTxInterval: 500000, MinRxInterval: 500000, Multiplier: 3
Remote: Disc: 2, Diag: 0, Demand: 0 Poll: 0
    MinTxInterval: 500000, MinRxInterval: 500000, Multiplier: 3
        Session Uptime: 0:17:49:14.100, LastSessionDownTimestamp: 0:0:0:0.0
Physical Port: TX: eth 1/17, RX: eth 1/17, Vlan Id: 1
Using PBIF Assist: Y

Registered Protocols (Protocol/VRFID): bgp/0
show bfd neighbors details
Displays detailed Bidirectional Forwarding Detection (BFD) neighbor information.

Syntax
`show bfd neighbors details [ ip-address | ipv6-address ]`

Parameters
- `ip-address`: Specifies the IP address of a neighbor.
- `ipv6-address`: Specifies the IPv6 address of a neighbor.

Modes
User EXEC mode

Command Output
The `show bfd neighbors details` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of Neighbor entries</td>
<td>Total number of BFD sessions.</td>
</tr>
<tr>
<td>NeighborAddress</td>
<td>IPv4 or IPv6 address of the remote peer.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the BFD session:</td>
</tr>
<tr>
<td></td>
<td>- UP</td>
</tr>
<tr>
<td></td>
<td>- DOWN</td>
</tr>
<tr>
<td></td>
<td>- A.DOWN - The administrative down state.</td>
</tr>
<tr>
<td></td>
<td>- INIT - The initialization state.</td>
</tr>
<tr>
<td></td>
<td>- UNKNOWN - The current state is unknown.</td>
</tr>
<tr>
<td>Interface</td>
<td>The logical port on which the peer is known.</td>
</tr>
<tr>
<td>Holddown</td>
<td>The interval in milliseconds after which the session will transition to the down state if no message is received.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in milliseconds at which the local device sends BFD messages to the remote peer.</td>
</tr>
<tr>
<td>R/H</td>
<td>R - Heard from Remote. Displays Y for Yes or N for No.</td>
</tr>
<tr>
<td></td>
<td>H - Hops. Display S for single hop or M for multihop.</td>
</tr>
<tr>
<td>Registered Protocols</td>
<td>Specifies which protocols are registered to use BFD on this port.</td>
</tr>
<tr>
<td>Local:</td>
<td>The local device</td>
</tr>
<tr>
<td>Disc</td>
<td>Value of the local discriminator field in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>Diag</td>
<td>Value of the diagnostic field in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>Demand</td>
<td>Value of the demand bit in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Poll</td>
<td>Value of the poll bit in the BFD control message as used by the local device in the last message sent.</td>
</tr>
<tr>
<td>MinTxInterval</td>
<td>The interval in milliseconds between which the device will send a BFD message from this local neighbor port to its peer.</td>
</tr>
<tr>
<td>MinRxInterval</td>
<td>The interval in milliseconds that the neighbor device waits to receive a BFD message from its peer on this local port.</td>
</tr>
<tr>
<td>Multiplier</td>
<td>The number of times that the neighbor device will wait for the MinRxInterval time on this port before it determines that its peer device is non-operational.</td>
</tr>
<tr>
<td>Remote:</td>
<td>Remote peer.</td>
</tr>
<tr>
<td>Disc</td>
<td>Value of the local discriminator field in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>Diag</td>
<td>Value of the diagnostic field in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>Demand</td>
<td>Value of the demand bit in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>Poll</td>
<td>Value of the poll bit in the BFD control message as received in the last message sent by the remote peer.</td>
</tr>
<tr>
<td>MinTxInterval</td>
<td>The interval in milliseconds between which the device will send a BFD message from the remote neighbor port to its peer.</td>
</tr>
<tr>
<td>MinRxInterval</td>
<td>The interval in milliseconds that the neighbor device waits to receive a BFD message from its peer on this remote port.</td>
</tr>
<tr>
<td>Multiplier</td>
<td>The number of times that the remote neighbor device will wait for the MinRxInterval time on this port before it determines that its peer device is non-operational.</td>
</tr>
<tr>
<td>Stats</td>
<td>Statistics</td>
</tr>
<tr>
<td>Rx</td>
<td>Total number of BFD control messages received from the remote peer.</td>
</tr>
<tr>
<td>Tx</td>
<td>Total number of BFD control messages sent to the remote peer.</td>
</tr>
<tr>
<td>SessionUpCount</td>
<td>The number of times the session has transitioned to the up state.</td>
</tr>
<tr>
<td>SysUpTime</td>
<td>The amount of time that the system has been up.</td>
</tr>
<tr>
<td>Session Uptime</td>
<td>The amount of time the session has been in the up state.</td>
</tr>
<tr>
<td>LastSessionDownTimestamp</td>
<td>The system time at which the session last transitioned from the up state to some other state.</td>
</tr>
<tr>
<td>Physical Port</td>
<td>The physical port on which the peer is known.</td>
</tr>
<tr>
<td>Vlan Id</td>
<td>The VLAN ID of the VLAN on which the physical port is resident</td>
</tr>
<tr>
<td>Session</td>
<td>Session details</td>
</tr>
<tr>
<td>Using PBIF Assist</td>
<td>Y for Yes: PBIF Assist is used for this BFD session.</td>
</tr>
<tr>
<td></td>
<td>N for No: PBIF is not used for this BFD session.</td>
</tr>
</tbody>
</table>
Examples

The following example displays detailed BFD neighbor information for the device.

device# show bfd neighbors details
Total number of Neighbor entries: 1
NeighborAddress                  State Interface   Holddown Interval  R/H
10.14.1.1                        UP    ve 50 300000 100000 Y/S
Registered Protocols(Protocol/VRFID): ospf/0
Local: Disc: 1, Diag: 0, Demand: 0 Poll: 0
   MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Remote: Disc: 22, Diag: 7, Demand: 0 Poll: 0
   MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Stats: RX: 72089 TX: 72101 SessionUpCount: 1 at SysUpTime: 0:1:30:54.775
   Session Uptime: 0:1:30:6.375, LastSessionDownTimestamp: 0:0:0:0.0
Physical Port: eth 4/1, Vlan Id: 50, Session: Active
Using PBIF Assist: Y
show bfd neighbors interface
Displays Bidirectional Forwarding Detection (BFD) neighbor information about specified interfaces.

Syntax

```
show bfd neighbors interface [ ethernet slot/port | pos slot/port | ve vlan-id | details ] [ ip-address | ipv6-address ]
```

Parameters

- **ethernet slot/port**: Specifies an Ethernet interface with a valid slot and port number.
- **pos slot/port**: Specifies a Packet over SONET (POS) interface with a valid slot and port number.
- **ve vlan-id**: Specifies a virtual Ethernet (VE) interface.
- **details**: Displays detailed neighbor interface information.
- **ip-address**: Specifies the IP address of a neighbor.
- **ipv6-address**: Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for the Ethernet 1/1 interface.

```
device# show bfd neighbors interface ethernet 1/1

BFD State: ENABLED Version: 1 Use PBIF Assist: Y SH setup delay 180 MH setup delay 0
Current Registered Protocols: mpls/0 ospf/2 ospf6/0 ospf/4 ospf/0
All Sessions: Current: 0 Maximum Allowed: 250 Maximum Exceeded Count: 0
Maximum TX/RX Sessions Allowed on LP: 80 Maximum Session Exceeded Count for LPs: 0
LP TX/Rx Sessions LP TX/Rx Sessions LP TX/Rx Sessions LP TX/Rx Sessions
 1 0/0 2 0/0 3 0/0 4 0/0
BFD Enabled ports count: 1
Port MinTx MinRx Mult Sessions
eth 1/1 55 55 5 0
```
show bfd neighbors isis

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for IS-IS.

Syntax

```
show bfd neighbors isis [ details ] [ ip-address | ipv6-address ]
```

Parameters

- **details**
  - Displays detailed neighbor interface information.
- **ip-address**
  - Specifies the IP address of a neighbor.
- **ipv6-address**
  - Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for IS-IS.

```
device# show bfd neighbors isis
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress State Interface Holddown Interval R/H
10.40.40.10 UP eth 3/6 900000 300000 Y/S
```

The following example displays detailed BFD neighbor information for IS-IS.

```
device# show bfd neighbors isis details
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress State Interface Holddown Interval R/H
10.40.40.10 UP eth 3/6 900000 300000 Y/S
Registered Protocols(Protocol/VRFID): isis/0
Local: Disc: 9, Diag: 0, Demand: 0 Poll: 0
  MinTxInterval: 300000, MinRxInterval: 300000, Multiplier: 3
Remote: Disc: 5, Diag: 0, Demand: 0 Poll: 0
  MinTxInterval: 300000, MinRxInterval: 300000, Multiplier: 3
  Session Uptime: 0:0:0:59.278, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 3/6,RX: eth 3/6,Vlan Id: 1
Using PBIF Assist: Y
```
show bfd neighbors ospf

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for OSPFv2.

Syntax

```
show bfd neighbors ospf [ details ] [ ip-address | ipv6-address ]
```

Parameters

- **details**
  Displays detailed neighbor interface information.
- **ip-address**
  Specifies the IP address of a neighbor.
- **ipv6-address**
  Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for OSPFv2:

```
device# show bfd neighbors ospf
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress  State  Interface   Holddown  Interval  R/H
1.1.1.1          UP     eth 1/2     300000     100000    Y/S
```

The following example displays detailed BFD neighbor information for OSPFv2:

```
device# show bfd neighbors ospf details
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress  State  Interface   Holddown  Interval  R/H
1.1.1.2          UP     eth 1/2     300000     100000    Y/S
Registered Protocols(Protocol/VRFID): static/0 ospf/0
Local: Disc: 1, Diag: 0, Demand: 0 Poll: 0
  MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Remote: Disc: 1, Diag: 0, Demand: 0 Poll: 0
  MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
  Session Uptime: 0:23:24:40.367, LastSessionDownTimestamp: 0:0:0:0.0
  Physical Port:TX: eth 1/2,RX: eth 1/2,Vlan Id: 1
  Using PBIF Assist: Y
```
show bfd neighbors ospf6
Displays Bidirectional Forwarding Detection (BFD) neighbor session information for OSPFv3.

Syntax

show bfd neighbors ospf6 [ details ] [ ip-address | ipv6-address ]

Parameters

details
Displays detailed neighbor interface information.

ip-address
Specifies the IP address of a neighbor.

ipv6-address
Specifies the IPv6 address of a neighbor.

Modes
User EXEC mode

Examples

The following example displays BFD neighbor information for OSPFv3.

device# show bfd neighbors ospf6

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress State Interface Holddown Interval R/H
fe80::21b:edff:fe3b:8601 UP eth 1/2 300000 100000 Y/S

The following example displays detailed BFD neighbor information for OSPFv3.

device# show bfd neighbors ospf6 details

Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress State Interface Holddown Interval R/H
fe80::21b:edff:fe3b:8601 UP eth 1/2 300000 100000 Y/S
Registered Protocols (Protocol/VRFID): ospf6/0
Local: Disc: 2, Diag: 0, Demand: 0 Poll: 0
MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Remote: Disc: 2, Diag: 0, Demand: 0 Poll: 0
MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Session Uptime: 0:23:16:8.793, LastSessionDownTimestamp: 0:0:0:0.0
Physical Port: TX: eth 1/2, RX: eth 1/2, Vlan Id: 1
Using PBIF Assist: Y
show bfd neighbors static

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for IP static routes.

Syntax

```
show bfd neighbors static [ details ] [ ip-address | ipv6-address ]
```

Parameters

details
Displays detailed neighbor interface information.

ip-address
Specifies the IP address of a neighbor.

ipv6-address
Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for IP static routes.

```
device# show bfd neighbors static
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress State Interface Holddown Interval  R/H
1.1.1.1       UP  eth 1/2      300000     100000    Y/S
```

The following example displays detailed BFD neighbor information for IP static routes.

```
device# show bfd neighbors static details
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress State Interface Holddown Interval  R/H
1.1.1.1       UP  eth 1/2      300000     100000    Y/S
Registered Protocols(Protocol/VRID): static/0 ospf/0
Local: Disc: 1, Diag: 0, Demand: 0 Poll: 0
MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Remote: Disc: 1, Diag: 0, Demand: 0 Poll: 0
MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Session Uptime: 0:23:25:49.719, LastSessionDownTimestamp: 0:0:0:0.0
Physical Port:TX: eth 1/2,RX: eth 1/2,Vlan Id: 1
Using PBIF Assist: Y
```
show bfd neighbors static6

Displays Bidirectional Forwarding Detection (BFD) neighbor session information for IPv6 static routes.

Syntax

```
show bfd neighbors static6 [ details ] [ ip-address | ipv6-address ]
```

Parameters

- `details`
  Displays detailed neighbor interface information.

- `ip-address`
  Specifies the IP address of a neighbor.

- `ipv6-address`
  Specifies the IPv6 address of a neighbor.

Modes

User EXEC mode

Examples

The following example displays BFD neighbor information for IPv6 static routes.

```
device# show bfd neighbors static6
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
NeighborAddress State Interface Holddown Interval R/H
1::1 UP eth 1/2 300000 100000 Y/S
```

The following example displays detailed BFD neighbor information for IPv6 static routes.

```
device# show bfd neighbors static6 details
Total Entries:1 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
Registered Protocols(Protocol/VRFID): static6/0
NeighborAddress State Interface Holddown Interval R/H
1::1 UP eth 1/2 300000 100000 Y/S
Remote: Disc: 3, Diag: 0, Demand: 0 Poll: 0
MinTxInterval: 100000, MinRxInterval: 100000, Multiplier: 3
Session Uptime: 0:23:11:58.266, LastSessionDownTimestamp: 0:0:0:0.0
Physical Port:TX: eth 1/2,RX: eth 1/2,Vlan Id: 1
Using PBIF Assist: Y
```
show bip slot

Displays a table that contains the lane number for a Physical Coding Sublayer (PCS) lane and a count of Bit Interleaved Parity (BIP) errors for that PCS lane, for each lane where a counter is active.

Syntax

```plaintext
show bip slot slot_number
```

Parameters

`slot_number`

Specifies the slot number for which the BIP information is to be displayed.

Modes

User EXEC mode.

Usage Guidelines

Command Output

The `show bip slot` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane</td>
<td>The PCS lane on the port.</td>
</tr>
<tr>
<td>Count</td>
<td>The value of the counter associated with the lane.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the `show bip slot` command:

device# show bip slot 3
Port 3/1:
PCS Lane BIP Error Counters :
*****************************
  Lane00 : 001     Lane01 : 001
  Lane02 : 001     Lane03 : 001
  Lane04 : 001     Lane05 : 001
  Lane06 : 001     Lane07 : 001
  Lane08 : 001     Lane09 : 001
  Lane10 : 001     Lane11 : 001
  Lane12 : 001     Lane13 : 001
  Lane14 : 001     Lane15 : 001
  Lane16 : 001     Lane17 : 001
  Lane18 : 001     Lane19 : 001
Port 3/2:
PCS Lane BIP Error Counters :
*****************************
  Lane00 : 000     Lane01 : 000
  Lane02 : 000     Lane03 : 000
  Lane04 : 000     Lane05 : 000
  Lane06 : 000     Lane07 : 000
  Lane08 : 000     Lane09 : 000
  Lane10 : 000     Lane11 : 000
  Lane12 : 000     Lane13 : 000
  Lane14 : 000     Lane15 : 000
  Lane16 : 000     Lane17 : 000
  Lane18 : 000     Lane19 : 000
All show BIP done

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00a</td>
<td>This command was modified</td>
</tr>
</tbody>
</table>

Netiron Command Line Interface (CLI) Reference Guide
S3-1004199-02
show cam-detail-eth

Displays Content Addressable Memory (CAM) programming information for a specific Layer 2 CAM flow entry.

Syntax

```
show cam-detail-eth slot/port mac_address [ vlan vlan_id | vpls-vlan vlan_id ]
```

Parameters

- **slot/port**: Specifies the LP module slot and port number.
- **mac_address**: Specifies the MAC address of the Layer 2 PRAM entry.
- **vlan vlan_id**: Specifies the VLAN ID number.
- **vpls-vlan vlan_id**: Specifies the VPLS-VLAN ID number.

Modes

Privileged EXEC level.

Usage Guidelines

Use this command to retrieve and display Layer 2 CAM or PRAM flow entry information without using a separate sequence of debugging commands. The command eliminates the need to remember indices information required to capture Layer 2 flow information by doing all the work in the back-end. The command only uses the MAC address or the VLAN ID or VPLS VLAN ID for Layer 2 to read and display information for a specific Layer 2 PRAM entry.

The command is supported only on the LP module.

**NOTE**

The command is supported on Brocade NetIron XMR Series and Brocade MLX Series devices.
Examples

The `show cam-detail-eth` command displays the following information on 2/8 with address fdab:1234:4567 of VLAN 100:

```
device# show cam-detail-eth 2/8 fdab:1234:4567 vlan 100

**************(show cam ethernet <slot/port>) output*************************
LP Index MAC            Age Port  IFL/ Out IF PRAM  Type
            (Hex)                         VLAN        (Hex)
2  4ffff ffff.ffff.0000 Dis 2/8   100    CPU    3ff5b DA

**************(dm cam [<interface> <index>]) output***************************
(CAM 0x00004ffff): ffff.ffff.0000/ffff.ffff.0000 VPN 0/0
**************(dm cam2pram <interface> <index>) output************************
(CAM2PRAM entry 0x09ffe): 0003ff5b cam idx: 0x0004ffff
(CAM2PRAM entry 0x09fff [MAC SA or Right IP]): 0003ff80
**************(dm pram <interface> <index> mac-da) output************************
127[00000000:00100000:8600800f:05f00000]0

*******PRAM MAC entry (DA)************
ALT SRC PORT    1          Use alternate src port
MONITOR         0          Copy packet to MONITOR port
CPU             0          Packet must be copied to CPU
DISCARD INVLD   0          Discard if lookup invalid
DISCARD PACKET  0          Force packet to be discarded
USE FID         1          Use FID from this PRAM entry
USE QOS ID      1          Use QOS ID for rate limiting
INNER VLAN VALID 0000    Inner Vlan Valid
QOS ID          0x20       QOS rate limiting ID
VALID           0x000000f   Per-port entry valid
FID             0x05f0      Forwarding ID
TRUNK ADJUST    0          Adjust FID based on trunk index
DIS_QOS_OVERRIDE 0         Disable QOS Override
PRIORITY_FORCE  0          Force pram priority to packet
PRIORITY        0          Packet priority
FASTPATH ENA    0          DA/SA is a known router
IDENT BLOCK     0          Ignore port or RX block
DPA KNOWN       0          DPA associated with this DA is known
US              0          Set RX_US bit
LOCAL ADDRESS   0          Address was learned locally
IGNORE US       0          Ignore router MAC
IGNORE ACLRES   0          Ignore ACL lookup
INNER VLAN      0000       Replacement Inner Vlan ID
PRAM TYPE       1          PRAM Entry Type
TRUNK ID        0          Trunk group ID
REPLACE VLAN    0          Use Outer Replacement VLAN ID
OUTER VLAN      0          Outer Replacement VLAN ID
MULTICAST VLAN  0          Set Multicast VLAN Flag
MATCH ALL DA    0          Match All DA Entry
LOCAL SWITCHING (MAC-DA only) 0          Perform L2 DA forwarding
DONT MODIFY PKT 0          Send Unmodified Copy
SOURCE PORT     0x00       Source Port of CAM entry
FPORT VALID     0x00       Host port per port entry valid
BOGUS LABEL BIT 0          Indicates if this label is used for single hop acct
TAG             0          VPLS Tag Mode support
NEXT HOP INDEX  0          next hop router index
PRAM MCAST SKIP MCAST 0      MCT/PBB mask indicating where to forward
PRAM EGRESS ID H1 0          higher 12-bits of PRAM_EGRESS_ID for HQOS support
PRAM EGRESS ID L0 0          Lower 4-bits of PRAM_EGRESS_ID for HQOS support
PUSH OUTER LABEL 0          Push the Outer Label
INNER LABEL 0      inner label
OUTER LABEL 0      outer label
REPLACE INNER VLAN 0      Use replacement inner VLAN

**************(dm fid-entry-table <fid>) output*******************************
FID 25 (000000019): cpu = 0, mcpu = (0, 0), num_write_not_needed = 0
  Slot0: 00000000 00000000
  Slot1: 00000000 00000000
  Slot2: 00000000 00000000
  Slot3: 00000000 00000000
  Slot4: 00000000 00000000
  Slot5: 00000000 00000000
  Slot6: 00000000 00000000
```
Slot7: 00000000 00000000
Slot8: 00000000 00000000
Slot9: 00000000 00000000
Slot10: 00000000 00000000
Slot11: 00000000 00000000
Slot12: 00000000 00000000
Slot13: 00000000 00000000
Slot14: 00000000 00000000
Slot15: 00000000 00000000
Slot16: 00000000 00000000
Slot17: 00000000 00000000
Slot18: 00000000 00000000
Slot19: 00000000 00000000
Slot20: 00000000 00000000
Slot21: 00000000 00000000
Slot22: 00000000 00000000
Slot23: 00000000 00000000
Slot24: 00000000 00000000
Slot25: 00000000 00000000
Slot26: 00000000 00000000
Slot27: 00000000 00000000
Slot28: 00000000 00000000
Slot29: 00000000 00000000
Slot30: 00000000 00000000
Slot31: 00000000 00000000
Slot32: 00000000 00000000

********************(dm statsram pram <slot/port> <index>) output***********************

(STATSRAM entry 0x03ff5b): pkt cnt: 217243, byte cnt: 32151964

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show cam-detail-ip
Displays Content Addressable Memory (CAM) programming information for a specific Layer 3 CAM flow entry.

Syntax
```
show cam-detail-ip slot/port ip_address/mask
```

Parameters
- **slot/port**
  Specifies the LP module slot and port number.
- **ip_address/mask**
  Specifies IP address and mask of the Layer 3 PRAM entry.

Modes
Privileged EXEC mode.

Usage Guidelines
Use this command to retrieve and display Layer 3 CAM or Parameter Random Access Memory (PRAM) flow entry information without using a separate sequence of debugging commands. The command eliminates the need to remember indices information required to capture Layer 3 flow information by doing all the work in the back-end. The command only uses the network IP address and mask to read and display information for a specific PRAM entry.

The command is supported only on the Line Processor (LP) module. The command is supported only for IPv4 CAM or PRAM flow entry. IPv6 CAM or PRAM is not supported. The output from the command displays only default Virtual Routing and Forwarding (VRF) flow information.

**NOTE**
The command is supported on Brocade NetIron XMR Series and Brocade MLX Series devices.
Examples

The `show cam-detail-ip` command displays the following information on 2/2 with address 1.1.1.1/24:

```
 device# show cam-detail-ip 2/2 1.1.1.1/24
 ****************************(show cam ip <ipaddr/mask>) output*****************************
 IP Address         MAC            Age IFL/ Out IF PRAM
 (Hex)                                          VLAN        (Hex)
2 01a8da(R) 1.1.1.0/24         0024.3892.4c01 Dis 1    2/2    3ff62
 ****************************(dm cam <interface> <index>) output**************************
(CAM 0x0001a8da left): 0.0.0.0/255.255.255.255
(CAM 0x0001a8da right): 1.1.1.0/255.255.255.0
 ****************************(dm cam2pram <interface> <index>) output********************
(CAM2PRAM entry 0x0351b4): 0003ffbb cam_idx: 0x0001a8da
(CAM2PRAM entry 0x0351b5 [MAC SA or Right IP]): 0003ff62
 ****************************(dm pram <interface> <index> ip) output********************
PRAM 0x3ff62 255[01770000:00000002:00000024:38924c01]128
127[60008003:00000000:0400000d:00190200]0
 ****************************PRAM IP entry ****************************
DA HIGH         0x0024     Replacement DA (high 2 bytes)
DA LOW          0x38924c01 Replacement DA (low 4 bytes)
VLAN_ID         0001       Replacement VLAN ID
MULTICAST_VLAN 0          Set multicast flag in packet header
REPLACE_VLAN_ID 1         Use replacement VLAN ID
SPA_DISCARD_PKT 0          If 1, allow RPF to discard the packet
MTU_CHECK       1          If 1, enforce mtu check
REPLACE_DA      1          Use replacement DA
IGNORE_SPA_MASK 0          If 1, Ignore SPA mask
MONITOR         0          Copy packet to MONITOR port
CPU             0          Packet must be copied to CPU
DISCARD INVALID 0          Discard if lookup invalid
DISCARD PACKET  0          Force packet to be discarded
USE FID         1          Use FID from this PRAM entry
USE QOS_ID      0          Use QOS ID for rate limiting
INNER_VLANVALID 0          Inner Vlan Valid
QOS_ID          0x00       QOS rate limiting ID
VALID           0x000000d  Per-port entry valid
FID             0x0019     Forwarding ID
TRUNK ADJUST    0          Adjust FID based on trunk index
PRIORITY_FORCE  0          PRIORITY
PRIORITY        0
FWD_COMMAND     2          L3 hardware forwarding command
USE TOS_ID      0          Use replacement TOS
TOS_ID          0x000      TOS replacement
IGNORE ACLRES   0          Ignore ACL lookup
VLAN_ID         0000       Replacement Inner VLAN ID
PRAM TYPE       0
TRUNK_ID        0
NEXTHOP_ROUTER INDEX 0x00000000
TNNL_MTO_CHK_L 1500
SRC_IPV4_ADDR/SPA MASK 0x00000002
GRE_TNNL_INGRESS 0
GRE_TNNL_EGRESS 0
GRE_ENFORC_SESSION_CHECK 0
6_TO_4_TNNL_INGRESS 0
6_TO_4_TNNL_EGRESS 0
6_TO_4_ENFORC_SESSION_CHECK 0
TNNL OUTER TOS  0
REPLACE INNER VLAN 0
 ****************************(dm statssram pram <slot/port> <index>) output**************
(STATSRAM entry 0x3ff62): pkt cnt: 118298, byte cnt: 1750810

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show cam ifl**

Displays CAM interface entries.

**Syntax**

```
show cam ifl slot/port
```

**Parameters**

`slot port`

Displays CAM interface entries for the specified port.

**Modes**

Privileged EXEC mode.

**Usage Guidelines**

Use this command to display IPv4 interface CAM entries, including local (port+VLAN+IP) and remote (VC+IP) entries.

**Command Output**

The `show cam ifl` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>Slot-number</td>
</tr>
<tr>
<td>Index (Hex)</td>
<td>Shows the row number of this entry in the IP route table.</td>
</tr>
<tr>
<td>Port</td>
<td>Port-number</td>
</tr>
<tr>
<td>Outer VLAN</td>
<td>Shows path</td>
</tr>
<tr>
<td>Inner VLAN</td>
<td>Shows channel</td>
</tr>
<tr>
<td>PRAM (Hex)</td>
<td>Shows the ACL PRAM entries.</td>
</tr>
<tr>
<td>IFL ID</td>
<td>Same as VPN-ID in IPVPN CAM</td>
</tr>
<tr>
<td>IPv4/v6 Routing</td>
<td>Shows whether IPv4 or IPv6 is enabled or disabled on the interface</td>
</tr>
</tbody>
</table>

**Examples**

The following examples displays CAM entries for interface 1/1.

```
device#show cam ifl 1/1
```

```
Slot  Index (Hex)  Port  Outer VLAN  Inner VLAN  PRAM (Hex)  IFL ID  IPv4/v6 Routing
4     0061fffd     1/2   1          0          001fffd  4097     0/0
4     0061ffff     1/1   1          0          001ffff  4097     1/0
```
To add VRF to VE.

Brocade(config)# vlan 22
Brocade(config-vlan-22)# tagged ethernet 1/7
Brocade(config-vlan-22)# router-interface ve 22
Brocade(config-vlan-22)# exit
Brocade(config)# interface ve 22
Brocade(config-vrf-22)# vrf forwarding blue
Brocade(config-vrf-22)# ip address 10.0.0.22/24
Brocade(config-vrf-22)# exit

device# show cam ifl 1/7
Slot Index Port Outer VLAN Inner VLAN PRAM IFL ID IPV4/V6 Routing
1 0061fff 1/7 22 0 001fff 4097
1/0
show cam ipvpn
Displays CAM VPN entries.

Syntax
```
show cam ipvpn slot/port
```

Parameters
```
slot port
```
Displays CAM VPN entries for the specified port.

Modes
Privileged EXEC mode

Usage Guidelines
Use this command to display IPv4 VPN CAM entries, including local (port+VLAN+IP) and remote (VC+IP) entries.

Command Output
The `show cam ipvpn` command displays the following information:

**TABLE 6 show cam ipvpn output**

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LP</td>
<td>Shows the number of the interface module.</td>
</tr>
<tr>
<td>Index (Hex)</td>
<td>Shows the row number of this entry in the IP route table.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the IP address of the interface.</td>
</tr>
<tr>
<td>In Port</td>
<td>Shows the port number.</td>
</tr>
<tr>
<td>In VLAN</td>
<td>Shows the VLAN number.</td>
</tr>
<tr>
<td>VPNID</td>
<td>Shows VPNID in the display.</td>
</tr>
<tr>
<td>In VC Lb</td>
<td>Shows VC label.</td>
</tr>
<tr>
<td>MAC</td>
<td>Shows the MAC address of the interface.</td>
</tr>
<tr>
<td>Age</td>
<td>Shows whether the age is enabled or disabled.</td>
</tr>
<tr>
<td>IFL VLAN</td>
<td>Shows the VLAN to which the port belongs.</td>
</tr>
<tr>
<td>IF</td>
<td>Shows the state of outgoing interface action.</td>
</tr>
<tr>
<td>PRAM (Hex)</td>
<td>Shows the ACL PRAM entries.</td>
</tr>
</tbody>
</table>
### Examples

The following example displays CAM entries for slot 1, port 7.

```plaintext
device# show cam ipvpn 1/7

<table>
<thead>
<tr>
<th>LP Index</th>
<th>IP Address</th>
<th>In</th>
<th>In</th>
<th>VPNID</th>
<th>In</th>
<th>MAC</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Hex)</td>
<td>Port</td>
<td>VLAN</td>
<td>VC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lb</td>
<td></td>
<td>In</td>
<td>N/A</td>
<td>N/A</td>
<td>In</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>Drop</td>
<td>N/A</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Dis</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Mgmt</td>
<td>N/A</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Drop</td>
<td>CPU</td>
<td>N/A</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>000a5</td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 308fa</td>
<td>10.0.0.0/32</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>1 308fb</td>
<td>10.0.0.255/32</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>1 308fc</td>
<td>10.0.0.22/32</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>1 308fd</td>
<td>192.168.1.0/32</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>1 308fe</td>
<td>192.168.1.255/32</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>1 308ff</td>
<td>192.168.1.1/32</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>1 3e566</td>
<td>10.0.0.0/24</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
<tr>
<td>1 3e567</td>
<td>192.168.1.0/24</td>
<td>N/A</td>
<td>4097</td>
<td>N/A</td>
<td>N/A</td>
<td>Dis</td>
<td></td>
</tr>
</tbody>
</table>

To add VRF to VE.
Brocade(config)# vlan 22
Brocade(config-vlan-22)# tagged ethe 1/7
Brocade(config-vlan-22)# router-interface ve 22
Brocade(config-vlan-22)# exit
Brocade(config)# interface ve 22
Brocade(config-vif-22)# vrf forwarding blue
Brocade(config-vif-22)# ip address 10.0.0.22/24
Brocade(config-vif-22)# exit

Brocade# show cam ipvvpn slot/port
```
show cam uda

Provides the details of the User Defined ACL (UDA) ACL CAM entry.

Syntax

```
show cam { uda } slot/port
```

Parameters

* slot/port
  Specifies the selected slot and port.

Modes

EXEC mode

Examples

The following example displays the output of the command.

```
device(config)# show cam uda 1/1
LP Index  VLAN UDA0      UDA1      UDA2      UDA3     Port  Action   PRAM
(Dec)                                                             (Dec)
1  057bfe 0    11223344  44556677  aabbccdd  0        1     Drop     7ff67
1  057c00 0    11223344  44556677  aabbccdd  0     0     Pass     7ff64
1  057c02 0    11223344  44556677  aabb      3333  0     Pass     7ff63
1  057c04 0    11223344  6677      aabb      aabb  0     Pass     7ff62
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show cluster

Displays information about the Multi-Chassis Trunking (MCT) clusters of the peer and client states.

Syntax

```
show cluster [ cluster ID [ ccp | client [ client RBridge ID | client name | disabled ] | client-health-check | l2vpn-peer | peer | vll ] |
cluster name [ ccp | client [ client RBridge ID | client name | disabled ] | client-health-check | l2vpn-peer | peer | vll ] | ccp
[ buffered_messages | peer ] | config [ begin | exclude | include ]
```

Parameters

- **cluster ID**
  Specifies the cluster ID.
  - **ccp**
    Specifies the MCT Cluster Communication Protocol (CCP) for the chosen cluster ID or cluster name.
  - **client**
    Specifies the cluster client information for the chosen cluster ID or cluster name.
    - **client RBridge ID**
      Specifies the client RBridge ID.
    - **client name**
      Specifies the cluster client name.
  - **disabled**
    Shows the MCT spoke PW state for CCEP ports.
  - **client-health-check**
    Specifies the cluster client health check information for the chosen cluster ID or cluster name.
  - **l2vpn-peer**
    Specifies the cluster L2VPN peer information for the chosen cluster ID or cluster name.
  - **peer**
    Specifies the cluster peer information for the chosen cluster ID or cluster name.
  - **vll**
    Specifies the cluster virtual leased line (VLL) information for the chosen cluster ID or cluster name.
  - **cluster name**
    Specifies the cluster name.
  - **ccp**
    Specifies the MCT CCP information.
  - **buffered_messages**
    Specifies the number of buffered CCP messages.
  - **peer**

Specifies the CCP peer information.

**config**

Specifies the MCT cluster configuration information.

**begin**

Specifies the output modifier by starting with the first matching line.

**exclude**

Specifies the output modifier by excluding the matching lines.

**include**

Specifies the output modifier by including the matching lines.

### Modes

- User EXEC mode
- Global configuration mode

### Usage guidelines

Information about the finite state machine (FSM) states that appear in the `show cluster` command output is provided in the following table.

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Up</td>
<td>With the CCP up, a client reaches this state when both local and remote MCT client configurations are deployed by way of the command line interface and the corresponding ports on both local and remote MCT peers are down.</td>
</tr>
<tr>
<td>Remote Up</td>
<td>With the CCP up, a client reaches this state on a peer when the ports belonging to the client are down on the local device and are up on the remote MCT peer.</td>
</tr>
<tr>
<td>Local Up</td>
<td>With the CCP up, a client reaches this state on an MCT peer when the ports belonging to the client reach the forwarding state in that device and the corresponding ports of this client in the remote MCT peer are down.</td>
</tr>
<tr>
<td>Up</td>
<td>With the CCP up, a client reaches this state when both the local and remote ports belonging to the client are up and are in the forwarding state.</td>
</tr>
</tbody>
</table>
The following example displays the peer and client state cluster information.

device# show cluster
Cluster CLUSTER-1 2000
---------------------
Cluster State: Deploy
Client Isolation Mode: Loose
Configured Member Vlan Range: 2 to 2000 2002 to 4090
Active Member Vlan Range: 2 to 3 21 to 148 201 404 to 445 501 to 508 2010 3511 to 3574 4021 to 4025 4051 4070 4080 4087 4090
ICL Info:
-------
Name Port Trunk
ICL-1 2/1 6
Peer Info:
--------
Peer IP: 1.1.1.1, Peer Rbridge Id: 1, ICL: ICL-1
KeepAlive Interval: 50 , Hold Time: 300, Fast Failover
Active Vlan Range: 2 to 3 21 to 148 201 404 to 445 501 to 508 2010 3511 to 3574 4021 to 4025 4051 4070 4080 4087 4090
Peer State: CCP Up (Up Time: 0 days:19 hr:24 min: 8 sec)
Client Info:
----------
Name    Rbridge-id     Config     Port  Trunk FSM-State
client-1   222        Deployed   1/2     3   Up
client-2   22        Deployed   1/40     -   Up

The following example displays MCT cluster information when the MCT admin state is up.

device(config)# cluster TOR 1
device(config-cluster-TOR)# show cluster

Cluster TOR 1
-----------
Rbridge Id: 2, Session Vlan: 4090
Cluster State: Deploy
Clients State: All client ports are administratively disabled
Client Isolation Mode: Loose
Cluster Mac Sync Mode: Enable, Mac sync Timer: 15 Min
Client Health Check Mode: Dynamic, Health Check Timer: 60 Sec
Configured Member Vlan Range: 2
Active Member Vlan Range: 2
Total Clients Configured : 2 ( Deployed Clients: 2)

ICL Info:
-------
Name Port Trunk
TOR 1/9 1

Peer Info:
--------
Peer IP: 1.1.1.1, Peer Rbridge Id: 1, ICL: TOR
KeepAlive Interval: 30 , Hold Time: 90, Fast Failover
Active Vlan Range: 2
Peer State: CCP Up (Up Time: 0 days: 0 hr:13 min:18 sec)

Client Info:
----------
Name    Rbridge-id     Config     Port  Trunk FSM-State
client-1   100        Deployed   1/6     3   Admin Up
client-2   200        Deployed   1/3     2   Admin Up
The following example displays MCT cluster information when the MCT remote state is up.

device(config)# cluster TOR 1
device(config-cluster-TOR)# client client-2
device(config-cluster-TOR-client-client-2)# show cluster

Cluster TOR 1
-------------
Rbridge Id: 1, Session Vlan: 4090
Cluster State: Deploy
Client Isolation Mode: Loose
Configured Member Vlan Range: 2
Active Member Vlan Range: 2
Total Clients Configured : 2 ( Deployed Clients: 2)

ICL Info:
--------
Name                  Port Trunk
TOR                   1/9   1

Peer Info:
----------
Peer IP: 1.1.1.2, Peer Rbridge Id: 2, ICL: TOR
KeepAlive Interval: 30 , Hold Time: 90, Fast Failover
Active Vlan Range: 2
Peer State: CCP Up (Up Time:   0 days: 0 hr:13 min: 8 sec)

Client Info:
------------
Name    Rbridge-id Config     Port  Trunk FSM-State
client-1 100        Deployed   1/3     2   Admin Up
client-2 200        Deployed   1/6     3   Remote Up

The following example displays MCT cluster information when the MCT local state is up.

device(config)# cluster TOR 1
device(config-cluster-TOR)# show cluster

Cluster TOR 1
-------------
Rbridge Id: 2, Session Vlan: 4090
Cluster State: Deploy
Client Isolation Mode: Loose
Configured Member Vlan Range: 2
Active Member Vlan Range: 2
Total Clients Configured : 2 ( Deployed Clients: 2)

ICL Info:
--------
Name                  Port Trunk
TOR                   1/9   1

Peer Info:
----------
Peer IP: 1.1.1.1, Peer Rbridge Id: 1, ICL: TOR
KeepAlive Interval: 30 , Hold Time: 90, Fast Failover
Active Vlan Range: 2
Peer State: CCP Up (Up Time:   0 days: 0 hr:13 min:18 sec)

Client Info:
------------
Name    Rbridge-id Config     Port  Trunk FSM-State
client-1 100        Deployed   1/6     3   Admin Up
client-2 200        Deployed   1/3     2   Local Up
The following example displays cluster client information when the MCT spoke pseudowire (PW) state is down for the L2VPN MCT Cluster Client Edge Port (CCEP).

```
device(config)# show cluster 1 client disabled
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Rbridge-id</th>
<th>Config</th>
<th>Port</th>
<th>Trunk</th>
<th>FSM-State</th>
<th>SpokePW-state</th>
</tr>
</thead>
<tbody>
<tr>
<td>R3</td>
<td>100</td>
<td>Deployed</td>
<td>3/3</td>
<td>3</td>
<td>Remote Up</td>
<td>Down</td>
</tr>
</tbody>
</table>

The following example displays the peer and client state cluster information and also identifies the LACP delay configured time of 5 seconds.

```
device#show cluster
Cluster mct 1
--------------------
Rbridge Id: 100, Session Vlan: 99
Cluster State: Deploy
Early sync of CCEP-UP info to MCT node enabled
lacp delay configured 5
Client Isolation Mode: Loose
Configured Member Vlan Range: 10
Active Member Vlan Range: 10
Total Clients Configured : 1 ( Deployed Clients: 1)

ICL Info:
---------
Name     Port Trunk
icl      2/6  2

Peer Info:
----------
Peer IP: 1.1.1.2, Peer Rbridge Id: 200, ICL: icl
KeepAlive Interval: 30, Hold Time: 90, Fast Failover
Active Vlan Range: 10
Peer State: CCP Up (Up Time: 0 days: 0 hr:19 min:12 sec)

Client Info:
------------
Name         Rbridge-id Config  Port | Trunk | FSM-State |
switch bridge 10 Deployed 3/13    3       Up      |
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include information about relevant FSM states.</td>
</tr>
<tr>
<td>6.0.00</td>
<td>This command was modified to include the disabled option for the show cluster client command. The command was also modified to include the LACP delay configured time value in the command output.</td>
</tr>
</tbody>
</table>
show configuration
Displays the router, switch, or firewall’s current configuration.

Syntax

```
show configuration
```

Modes

EXEC mode.

Usage Guidelines

The outbound-fec filter configuration parameter now records in the startup or running configuration. It also now displays the name of the prefix-list configured in the LDP for outbound FEC filtering.

The outbound-fec filter configuration parameter is recorded in the startup or running configuration.

This command operates in all modes.

Examples

The following example displays output containing additional information indicating configured link protection:

```
device> show mpls conf
router mpls
    ..... lsp 1
to 44.44.44.44
  adaptive
  frr
  link-protection
  enable
```

The following example displays output when there is no request for link protection:

```
device> show mpls conf
router mpls
    ..... lsp 1
to 44.44.44.44
  adaptive
  frr
  enable
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>The outbound-fec filter configuration parameter is recorded in the startup or running configuration. The output of this command now contains additional information indicating link protection is configured.</td>
</tr>
</tbody>
</table>
show cpu histogram

Displays task CPU usage information, including the percentage, and total percentage of the CPU utilization of a task histogram at 1, 5, and 10 second average duration.

Syntax

show cpu histogram { hold | wait | interrupt | timer } [ above threshold-value | noclear | taskname name ]
show cpu histogram { util-10s | util-1s | util-5s } [ above threshold-value | noclear | taskname name ]
show cpu histogram { util-all-10s | util-all-1s | util-all-5s } [ above threshold-value | noclear ]

Parameters

hold
    Specifies the display of task hold time information.

wait
    Specifies the display of task wait time information.

interrupt
    Specifies the display of task user-interrupt usage information.

timer
    Specifies the display of task sys-timer time usage information.

util-10s
    Specifies the CPU utilization per task histogram at a 10 second average duration.

util-1s
    Specifies the CPU utilization per task histogram at a 1 second average duration.

util-5s
    Specifies the CPU utilization per task histogram at a 5 second average duration.

util-all-10s
    Specifies the total CPU utilization of a task histogram at a 10 second average duration.

util-all-1s
    Specifies the total CPU utilization of a task histogram at a 1 second average duration.

util-all-5s
    Specifies the total CPU utilization of a task histogram at a 5 second average duration.

above threshold-value
    Specifies the display of histogram information for tasks whose maximum hold time is above the specified value.

noclear
    Specifies that histogram data should not be cleared after display. By default, information is cleared on read.

taskname name
    Specifies the display of histogram information for a specific task.
**Show Commands**

**Modes**

User EXEC mode

**Usage Guidelines**

Use the command to display the task CPU usage information.

Use the `show cpu histogram { util-10s | util-1s | util-5s }` command to display the CPU percentage of a task histogram utilizing high CPU conditions at 1, 5, and 10 second durations.

To display the total CPU unitization of a task histogram at 1, 5, and 10 second average duration, use the `show cpu histogram { util-all-10s | util-all-1s | util-all-5s }` command. This command is supported on the management module and the interface module. The CPU percent utilization and time stamps are displayed for the durations.

Tasks that may use high CPU utilization include packet burst in the interface module, multiple protocols flapping at the same time, a protocol task in a wrong state that keeps the CPU busy, and high route processing that causes high CPU conditions in the management module and interface module CPUs.

**Command Output**

The `show cpu histogram` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of bucket</td>
<td>The task run time that is divided into interval buckets. For example, bucket 1(0-50ms), bucket 2 (50-100ms), and bucket 3(100-150ms).</td>
</tr>
<tr>
<td>Bucket Granularity</td>
<td>The bucket granularity is 5%. Each bucket contains values within 5% of range. For example, bucket 1 contains values 0-4, bucket 2 contains values 5-9, and so on.</td>
</tr>
<tr>
<td>Last Cleared at</td>
<td>The time at which the values are cleared last.</td>
</tr>
<tr>
<td>No of Task</td>
<td>The total number of tasks running in the system at a time.</td>
</tr>
<tr>
<td>Task Name</td>
<td>The name of the task displayed.</td>
</tr>
<tr>
<td>BktNum</td>
<td>The bucket number -1,2, or 3 that corresponds with the value it belongs to.</td>
</tr>
<tr>
<td>Bkt Value (%)</td>
<td>The time range of the bucket.</td>
</tr>
<tr>
<td>No of Time</td>
<td>The number of times the value in the bucket range is utilizing CPU. For example, task, sfm_mgr, was using the CPU in the range of 10-15, at 83 times.</td>
</tr>
<tr>
<td>CPU Util Total (%)</td>
<td>The total CPU utilization of a task.</td>
</tr>
<tr>
<td>Util Time Max</td>
<td>The maximum CPU utilization value of a bucket.</td>
</tr>
<tr>
<td>Time</td>
<td>The time stamp of the most recent CPU utilization for a particular task.</td>
</tr>
</tbody>
</table>
Examples

The following example displays task hold time information:

device# show cpu histogram hold
HISTOGRAM CPU HISTOGRAM INFO
-----------------------------------------------
  No of Bucket : 51
  Bucket Granularity : 10 ms
  Last cleared at : 2012.07.10-07:29:20.704
  No of Task : 67

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Bkt Num</th>
<th>Bkt Time(ms)</th>
<th>No of Time</th>
<th>HoldTime Total(s)</th>
<th>HoldTime Max(ms)</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_rx</td>
<td>1</td>
<td>000-010</td>
<td>4</td>
<td>.000463</td>
<td>.201</td>
<td>2012.07.10-07:29:20.701</td>
</tr>
<tr>
<td>vlan</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000025</td>
<td>.025</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>mac_mgr</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000010</td>
<td>.010</td>
<td>2012.07.10-07:29:20.701</td>
</tr>
<tr>
<td>mrp</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000025</td>
<td>.025</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>erp</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000025</td>
<td>.025</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>mxrp</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000009</td>
<td>.009</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>rtm</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000062</td>
<td>.062</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>rtm6</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000091</td>
<td>.091</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>ip_tx</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000207</td>
<td>.207</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>l2vpn</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.00018</td>
<td>.018</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>ospf</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000465</td>
<td>.046</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>isis</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000012</td>
<td>.009</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>mcast</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000025</td>
<td>.017</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>ospf6</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.00012</td>
<td>.012</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>mcast6</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.00029</td>
<td>.012</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>web</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000029</td>
<td>.012</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>lacp</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.00013</td>
<td>.013</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>loop_detect</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.000009</td>
<td>.009</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>cluster_mgr</td>
<td>1</td>
<td>000-010</td>
<td>1</td>
<td>.00011</td>
<td>.011</td>
<td>2012.07.10-07:29:20.700</td>
</tr>
<tr>
<td>telnet_0</td>
<td>1</td>
<td>000-010</td>
<td>4</td>
<td>.003</td>
<td>3</td>
<td>2012.07.10-07:29:20.672</td>
</tr>
</tbody>
</table>

The following example displays the CPU utilization of a task histogram at a 5 second average duration.

device# show cpu histogram util-5s
HISTOGRAM CPU UTIL PER TASK INFO (5sec average)
-----------------------------------------------
  No of Bucket : 21
  Bucket Granularity : 5%
  No of Task : 72

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Bkt Num</th>
<th>Bkt Value(%)</th>
<th>No of Time</th>
<th>CPU Util Total(%)</th>
<th>Util Max(%)</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$flash</td>
<td>1</td>
<td>000-005</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>2014.09.10-01:08:29.500</td>
</tr>
<tr>
<td>$flash</td>
<td>2</td>
<td>005-010</td>
<td>17</td>
<td>7</td>
<td>7</td>
<td>2014.09.14-05:28:22.450</td>
</tr>
<tr>
<td>main</td>
<td>1</td>
<td>000-005</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2014.09.04-18:18:44.350</td>
</tr>
<tr>
<td>ip_rx</td>
<td>1</td>
<td>000-005</td>
<td>18</td>
<td>1</td>
<td>1</td>
<td>2014.09.14-21:03:19.850</td>
</tr>
<tr>
<td>ip_rx</td>
<td>2</td>
<td>005-010</td>
<td>1</td>
<td>37</td>
<td>7</td>
<td>2014.09.05-02:00:13.050</td>
</tr>
<tr>
<td>console</td>
<td>1</td>
<td>000-005</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>2014.09.15-11:32:08.400</td>
</tr>
<tr>
<td>console</td>
<td>2</td>
<td>005-010</td>
<td>1</td>
<td>17</td>
<td>8</td>
<td>2014.09.04-18:18:44.350</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show cpu histogram sequence
Displays sequential execution of CPU task information.

Syntax

```
show cpu histogram sequence [ taskname name | above threshold-value | trace ]
```

Parameters

- **sequence**
  Specifies the display of sequential execution of CPU task information.
- **taskname name**
  Specifies the display of histogram information for a specific CPU task.
- **above threshold-value**
  Specifies the display of histogram information for CPU tasks whose maximum hold time is above the specified value.
- **trace**
  Specifies the display of high CPU condition task trace information.

Modes

User EXEC mode
Examples

The following example displays sequential execution of CPU task information:

device# show cpu histogram sequence

HISTOGRAM TASK SEQUENCE INFO

<table>
<thead>
<tr>
<th>Seq No</th>
<th>Task Name</th>
<th>Context</th>
<th>HoldTime</th>
<th>Start Time</th>
<th>End Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:33:08.790</td>
<td>07:33:08.806</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>2</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:33:08.772</td>
<td>07:33:08.789</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>3</td>
<td>snms</td>
<td>TASK</td>
<td>17</td>
<td>07:33:08.755</td>
<td>07:33:08.772</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>4</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:23:08.790</td>
<td>07:23:08.806</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>5</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:23:08.772</td>
<td>07:23:08.789</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>6</td>
<td>snms</td>
<td>TASK</td>
<td>17</td>
<td>07:23:08.755</td>
<td>07:23:08.772</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>7</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:13:08.790</td>
<td>07:13:08.806</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>8</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:13:08.772</td>
<td>07:13:08.789</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>9</td>
<td>snms</td>
<td>TASK</td>
<td>17</td>
<td>07:13:08.755</td>
<td>07:13:08.772</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>10</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:03:08.790</td>
<td>07:03:08.806</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>11</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>07:03:08.772</td>
<td>07:03:08.789</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>12</td>
<td>snms</td>
<td>TASK</td>
<td>17</td>
<td>07:03:08.755</td>
<td>07:03:08.772</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>13</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>06:53:08.790</td>
<td>06:53:08.806</td>
<td>2012.07.10</td>
</tr>
<tr>
<td>14</td>
<td>telnet_0</td>
<td>TASK</td>
<td>50</td>
<td>09:51:50.091</td>
<td>09:51:50.142</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>15</td>
<td>telnet_0</td>
<td>TASK</td>
<td>50</td>
<td>09:51:35.184</td>
<td>09:51:35.234</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>16</td>
<td>console</td>
<td>TASK</td>
<td>50</td>
<td>09:51:11.451</td>
<td>09:51:11.501</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>17</td>
<td>telnet_0</td>
<td>TASK</td>
<td>50</td>
<td>09:47:01.459</td>
<td>09:47:01.509</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>18</td>
<td>console</td>
<td>TASK</td>
<td>52</td>
<td>09:46:32.443</td>
<td>09:46:32.496</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>19</td>
<td>mpls</td>
<td>TIMER</td>
<td>12</td>
<td>09:46:32.428</td>
<td>09:46:32.441</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>20</td>
<td>telnet_0</td>
<td>TASK</td>
<td>54</td>
<td>09:46:03.018</td>
<td>09:46:03.072</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>21</td>
<td>telnet_0</td>
<td>TASK</td>
<td>52</td>
<td>09:44:31.749</td>
<td>09:44:31.802</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>22</td>
<td>telnet_0</td>
<td>TASK</td>
<td>50</td>
<td>09:44:17.984</td>
<td>09:44:18.034</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>23</td>
<td>telnet_0</td>
<td>TASK</td>
<td>50</td>
<td>09:43:43.638</td>
<td>09:43:43.689</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>34</td>
<td>telnet_0</td>
<td>TASK</td>
<td>12</td>
<td>09:43:43.623</td>
<td>09:43:43.636</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>35</td>
<td>telnet_0</td>
<td>TASK</td>
<td>54</td>
<td>09:43:20.669</td>
<td>09:43:20.724</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>36</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>09:43:08.740</td>
<td>09:43:08.756</td>
<td>2012.07.05</td>
</tr>
<tr>
<td>37</td>
<td>snms</td>
<td>TASK</td>
<td>16</td>
<td>09:43:08.723</td>
<td>09:43:08.740</td>
<td>2012.07.05</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>R05.5.00</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>
**show dot1x-mka group**

Shows details for the specified MACsec Key Agreement (MKA) groups configured on this device, or for a designated MKA group.

**Syntax**

```
show dot1x-mka group group-name
```

**Parameters**

- **group-name**
  Limits the group configuration displayed to the named MKA group.

**Modes**

EXEC or Privileged EXEC mode

**Command Output**

The `show dot1x-mka group` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x-mka group</td>
<td>The configuration details that follow are for the specified MACsec MKA group.</td>
</tr>
<tr>
<td>key-server-priority</td>
<td>The key server priority value used by MKA protocol for electing the key server.</td>
</tr>
<tr>
<td>macsec cipher-suite gcm-aes-128</td>
<td>MACsec transmissions are encrypted.</td>
</tr>
<tr>
<td>or macsec cipher-suite gcm-aes-128 integrity-only</td>
<td>or ICV checking only is performed.</td>
</tr>
<tr>
<td>macsec confidentiality-offset</td>
<td>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).</td>
</tr>
<tr>
<td>macsec frame-validation {check</td>
<td>discard}</td>
</tr>
<tr>
<td>macsec replay-protection {strict</td>
<td>out-of-order window-size size}</td>
</tr>
</tbody>
</table>

**Capability**
Examples

The following example lists the configuration details for MKA group test1.

Brocade(config-dot1x-mka)#show dot1x-mka group group1
Brocade Group name group1
    Key Server Priority : 16
    Cipher Suite      : gcm-aes-128
    Capability        : Integrity, Confidentiality with offset
    Confidentiality Offset : 0
    Frame Validation  : strict
    Replay Protection : strict

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show dot1x-mka config

Shows the MACsec Key Agreement (MKA) configuration for the device.

Syntax

```
show dot1x-mka config
```

Modes

User EXEC mode

Usage Guidelines

Default configuration is not displayed when this command is executed.

Command Output

The `show dot1x-mka config` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x-mka-enable</td>
<td>MACsec is enabled on the device.</td>
</tr>
<tr>
<td>enable-mka ethernet slot/port</td>
<td>The ethernet interfaces specified are enabled for MACsec.</td>
</tr>
<tr>
<td>mka-cfg-group group-name</td>
<td>The configuration details that follow are for the named MACsec MKA group.</td>
</tr>
<tr>
<td>key-server-priority value</td>
<td>The key server priority value used by MKA protocol for electing the key server.</td>
</tr>
<tr>
<td>macsec confidentiality-offset value</td>
<td>The byte offset used for encrypted data is set to the value shown. ALLOWABLE values are 30 (the first 30 bytes of data are not encrypted), and 50 (the first 50 bytes of data are not encrypted).</td>
</tr>
<tr>
<td>macsec frame-validation { check</td>
<td>discard }</td>
</tr>
<tr>
<td>macsec-replay protection { strict</td>
<td>out-of-order window-size value }</td>
</tr>
<tr>
<td>pre-shared-key value key-name value</td>
<td>The pre-shared key is set to this value and name for the MKA configuration group. Both key and name are hexadecimal strings.</td>
</tr>
</tbody>
</table>
Examples

The following example displays MACsec configuration information on Brocade device with MACsec enabled.

```
Brocade(config-dot1x-mka)#show dot1x-mka config
dot1x-mka-enable
  mka-cfg-group group1
    key-server-priority 20
    macsec frame-validation check
    macsec confidentiality-offset 30
    macsec replay-protection out-of-order window-size 100
  mka-cfg-group group2

  enable-mka ethernet 1/1 to ethernet 1/9
    mka-cfg-group group1
      pre-shared-key 0102030405060708090A0B0C0D0E0F10 key-name 11223344
    enable-mka ethernet 1/10
      mka-cfg-group group1
        pre-shared-key 0505030405060708090A0B0C0D0E0F10 key-name 55667788
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show dot1x-mka sessions brief
Displays a brief summary of all MACsec Key Agreement (MKA) sessions on the device.

Syntax

show dot1x-mka sessions brief

Modes

User EXEC mode

Command Output

The show dot1x-mka sessions command with the brief option displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Designates the interface for which MACsec information is listed (by device, slot, and port).</td>
</tr>
<tr>
<td>Link-Status</td>
<td>Indicates whether the link is up or down.</td>
</tr>
<tr>
<td>MKA-Status</td>
<td>Indicates whether a secure channel has been established.</td>
</tr>
<tr>
<td>Key-Server</td>
<td>Indicates whether the interface is operating as a key-server.</td>
</tr>
<tr>
<td>Negotiated Capability</td>
<td>Indicates MACsec parameters negotiated on the designated interface.</td>
</tr>
</tbody>
</table>

Examples

In the following example, all enabled MKA interfaces on the device are listed, along with configured parameters and current status.

device(config-dot1x-mka)# show dot1x-mka sessions brief

<table>
<thead>
<tr>
<th>Port</th>
<th>Link-Status</th>
<th>Secured</th>
<th>Key-Server</th>
<th>Negotiated Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/2</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
<tr>
<td>4/3</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
<tr>
<td>4/4</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
<tr>
<td>4/7</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
<tr>
<td>4/11</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
<tr>
<td>4/12</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
<tr>
<td>4/17</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
<tr>
<td>4/18</td>
<td>Up</td>
<td>Yes</td>
<td>Yes</td>
<td>Integrity, Confidentiality with offset 0</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show dot1x-mka sessions ethernet**

Displays a summary of all MACsec Key Agreement (MKA) sessions on the device.

**Syntax**

```
show dot1x-mka sessions [ ethernet slot / port ]
```

**Parameters**

- `ethernet slot / port`
  Displays MKA sessions that are active on a specified Ethernet interface. The Ethernet interface is specified by slot on the device, and interface on the slot.

**Modes**

User EXEC mode

**Command Output**

The `show dot1x-mka sessions` command with the `ethernet` interface options displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The information that follows applies to the designated interface.</td>
</tr>
<tr>
<td>DOT1X-MKA Enabled (Yes, No)</td>
<td>Indicates whether MKA is enabled for the designated interface.</td>
</tr>
<tr>
<td>DOT1X-MKA Active (Yes, No)</td>
<td>Indicates whether MKA is active on the interface.</td>
</tr>
<tr>
<td>Key Server (Yes, No)</td>
<td>Indicates whether the MKA key-server is active over the interface.</td>
</tr>
<tr>
<td><strong>Configuration Status:</strong></td>
<td>The following fields describe the MKA configuration applied to the interface.</td>
</tr>
<tr>
<td>Enabled (Yes, No)</td>
<td>Indicates whether MACsec is currently enabled.</td>
</tr>
<tr>
<td>Group name</td>
<td>MKA configuration group that has been associated with the interface.</td>
</tr>
<tr>
<td>Capability (Integrity and or confidentiality)</td>
<td>Indicates whether ICV checks are being performed on MACsec frames and whether encryption is being applied.</td>
</tr>
<tr>
<td>Confidentiality offset</td>
<td>Specifies the offset value set.</td>
</tr>
<tr>
<td>Desired (Yes, No)</td>
<td>Indicates whether port is interested in securing the communication using MACsec.</td>
</tr>
<tr>
<td>Protection (Yes, No)</td>
<td>Indicates whether replay protection is applied to the interface.</td>
</tr>
<tr>
<td>Validation</td>
<td>Indicates whether frames received are being checked for valid MACsec headers.</td>
</tr>
<tr>
<td>Replay Protection (Strict, Out of Order)</td>
<td>Indicates that replay protection is configured and whether frames must be received in exact order or within an allowable window.</td>
</tr>
<tr>
<td>Replay Protection Size</td>
<td>Indicates the allowable window size within which frames may be received.</td>
</tr>
<tr>
<td>Cipher Suite (GCM-AES-128)</td>
<td>Specifies the cipher suite used for ICV checking, encryption, and decryption.</td>
</tr>
<tr>
<td>Authenticator</td>
<td></td>
</tr>
<tr>
<td>Key Server Priority</td>
<td>Specifies the key-server priority configured on the interface.</td>
</tr>
<tr>
<td>Algorithm Agility</td>
<td></td>
</tr>
<tr>
<td>CAK NAME</td>
<td></td>
</tr>
<tr>
<td><strong>Secure Channel Information(SCI)</strong></td>
<td>The following fields describe a secure channel established on this interface.</td>
</tr>
<tr>
<td>Actor SCI</td>
<td>Provides the hexadecimal value of the Secure Channel Identifier for this channel.</td>
</tr>
<tr>
<td>Actor Priority</td>
<td></td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Key Server SCI</td>
<td></td>
</tr>
<tr>
<td>Key Server Priority</td>
<td></td>
</tr>
<tr>
<td><strong>Logon Status:</strong></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Authenticated</td>
<td></td>
</tr>
<tr>
<td>Secured</td>
<td></td>
</tr>
<tr>
<td>Failed</td>
<td></td>
</tr>
<tr>
<td><strong>Latest Kl, KN and AN Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Latest Kl</td>
<td></td>
</tr>
<tr>
<td>Tx Key Number</td>
<td></td>
</tr>
<tr>
<td>Rx Key Number</td>
<td></td>
</tr>
<tr>
<td>Tx Association Number</td>
<td></td>
</tr>
<tr>
<td>Rx Association Number</td>
<td></td>
</tr>
<tr>
<td><strong>Participant Information:</strong></td>
<td></td>
</tr>
<tr>
<td>SCI</td>
<td></td>
</tr>
<tr>
<td>Key Identifier</td>
<td>Provides the MACsec number assigned to the MKA peer.</td>
</tr>
<tr>
<td>Member Identifier</td>
<td>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.</td>
</tr>
<tr>
<td>Message Number</td>
<td></td>
</tr>
<tr>
<td>CKN</td>
<td></td>
</tr>
<tr>
<td>Key Length(in bytes)</td>
<td></td>
</tr>
<tr>
<td><strong>Secure Channel Information:</strong></td>
<td></td>
</tr>
<tr>
<td>No. of Peers (Live and Potential)</td>
<td></td>
</tr>
<tr>
<td>Latest SAK Status</td>
<td>Indicates the Secure Association Key (SAK) state.</td>
</tr>
<tr>
<td>Negotiated Capability (Integrity and or Confidentiality with offset)</td>
<td>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.)</td>
</tr>
</tbody>
</table>

The output fields that follow provide information on actual and potential MACsec peer interfaces

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State (Live or Potential)</td>
<td>Indicates whether the peer is considered a live peer or a potential peer for MKA protocol.</td>
</tr>
<tr>
<td>Member Identifier</td>
<td>Designates the peer by its Member Identifier, a hexadecimal value.</td>
</tr>
<tr>
<td>Message Number</td>
<td>Provides the Message Number that appears in Hello packets from the designated peer interface as a hexadecimal value.</td>
</tr>
<tr>
<td>SCI</td>
<td>Provides the peer’s Secure Channel Identifier.</td>
</tr>
<tr>
<td>Priority</td>
<td>Provides the key-server priority configured on the peer interface.</td>
</tr>
</tbody>
</table>
Examples

The following example lists MKA sessions that are active on Ethernet interface 4/1, with configuration details for each active interface.

Brocade(config)#show dot1x-mka sessions ethernet 4/1

Interface : 4/1
DOT1X-MKA Enabled : Yes
DOT1X-MKA Active : Yes

Configuration Status:
Group Name : 1
Capability : Integrity, Confidentiality with offset
Confidentiality offset : 0
Desired : Yes
Protection : Yes
Validation : Strict
Replay Protection : None
Replay Protection Size : 0
Cipher Suite : GCM-AES-128

Authenticator : No
Key Server Priority : 16
Algorithm Agility : 80C201

CAK NAME : 11223344

SCI Information:
Actor SCI : 0024388f6b900001
Actor Priority : 16
Key Server SCI : 0024388f6b900001
Key Server Priority : 16

MKA Status:
Enabled : Yes
Authenticated : No
Secured : Yes
Failed : No

Latest KI, KN and AN Information:
Latest KI : 42b4d71d520263cad8727d91000000001
Tx Key Number : 1
Rx Key Number : 0
Tx Association Number : 0
Rx Association Number : 0

Participant Information:
SCI : 0024388f6b900001
Key Identifier : 1
Member Identifier : 42b4d71d520263cad8727d91
Message Number : 3491
CKN Name : 11223344
Key Length (in bytes) : 16

Secure Channel Information:
No. of Peers (Live and Potential) : 1
Latest SAK Status : Rx & TX
Negotiated Capability : Integrity, Confidentiality with offset 0

Peer Information (Live and Potential):
State Member Identifier Message Number SCI Priority Capability
----- --------------- ---- ---------- ----------
Live 66dfa9b5037a9c7aa8b5c71e 3490 0024389e2d300001 16 2
**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show dot1x-mka statistics**

Displays current MACsec Key Agreement (MKA) statistics on the interface.

**Syntax**

```
show dot1x-mka statistics ethernet slot/port
```

**Parameters**

- **ethernet slot/port**
  
  Ethernet interface for which MKA statistics are to be displayed. The interface is designated by a slot on the device and interface on the slot.

**Modes**

EXEC or Privileged EXEC mode

**Usage Guidelines**

It is recommended that you use the `clear dot1x-mka statistics` command to clear results of the previous `show dot1x-mka statistics` command before re-executing it.

**Command Output**

The `show dot1x-mka statistics` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface (slot/port)</td>
<td>The output fields describe MACsec activity for the designated interface.</td>
</tr>
<tr>
<td>MKA in Pkts</td>
<td>MKA protocol packets received</td>
</tr>
<tr>
<td>MKA in SAK Pkts</td>
<td>MKA protocol packets received containing a SAK</td>
</tr>
<tr>
<td>MKA in Bad Pkts</td>
<td>MKA protocol packets received that are bad</td>
</tr>
<tr>
<td>MKA in Bad ICV Pkts</td>
<td>MKA protocol packets received with a bad ICV</td>
</tr>
<tr>
<td>MKA in Mismatch Pkts</td>
<td>MKA protocol packets received with mismatched CAK</td>
</tr>
<tr>
<td>MKA out Pkts</td>
<td>MKA protocol packets transmitted</td>
</tr>
<tr>
<td>MKA out SAK Pkts</td>
<td>MKA protocol packets transmitted containing a SAK</td>
</tr>
</tbody>
</table>
Examples

The following example shows MKA statistics for Ethernet interface 3/2, which is transmitting and receiving MACsec frames.

Brocade(config)# show dot1x-mka statistics ethernet 3/2

<table>
<thead>
<tr>
<th>Interface</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3/2</td>
</tr>
<tr>
<td>MKA in Pkts</td>
<td>89858</td>
</tr>
<tr>
<td>MKA in SAK Pkts</td>
<td>0</td>
</tr>
<tr>
<td>MKA in Bad Pkts</td>
<td>0</td>
</tr>
<tr>
<td>MKA in Bad ICV Pkts</td>
<td>0</td>
</tr>
<tr>
<td>MKA in Mismatch Pkts</td>
<td>0</td>
</tr>
<tr>
<td>MKA out Pkts</td>
<td>90225</td>
</tr>
<tr>
<td>MKA out SAK Pkts</td>
<td>192</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show egress-truncate

Displays the configuration details for the egress-truncate command.

Syntax

show egress-truncate
show egress-truncate interface slot/port

Parameters

interface

Displays the configuration of the ports in a slot determined by the slot/port variable.

Modes

This command operates under all modes.

Command Output

The show egress-truncate interface command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SlotNo</td>
<td>The slot number where egress-truncate has been applied.</td>
</tr>
<tr>
<td>Device-id</td>
<td>The device ID of where egress-truncate has been applied.</td>
</tr>
<tr>
<td>Size</td>
<td>The configured size of the egress truncated packet.</td>
</tr>
<tr>
<td>Status</td>
<td>The status (enabled or disabled) for the specified interface.</td>
</tr>
</tbody>
</table>

Examples

The following example displays the show egress-truncate command:

device#show egress-truncate
SlotNo Device-id Size Status
1 1 100 Enabled
2 2 90  Enabled
3 1 64  Enabled
Enabled Ports: e 10/1
device#

The following example displays the show egress-truncate interface command:

device#show egress-truncate interface 10/1
Device status : Enabled
Egress Truncate Packet Size:200
Port Status: Enabled
device#

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show ikev2 policy**
Displays configuration information about Internet Key Exchange version 2 (IKEv2) policies.

**Syntax**
```
show ikev2 policy [ policy-name ]
```

**Parameters**

`policy-name`
Specifies the name of an IKEv2 policy.

**Modes**
User EXEC mode

**Usage Guidelines**
This command may be entered in all configuration modes.

When a policy is not specified, this command displays information about all IKEv2 policies.

**Command Output**
The `show ikev2 policy` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of an IKEv2 policy.</td>
</tr>
<tr>
<td>vrf</td>
<td>The front-door VRF (fvrf) to match for the policy.</td>
</tr>
<tr>
<td>Local address/Mask</td>
<td>The local IP address to match for the policy.</td>
</tr>
<tr>
<td>Proposal</td>
<td>The IKEv2 proposal that is configured for the policy.</td>
</tr>
</tbody>
</table>

**Examples**
The following example displays information about all configured IKEv2 policies.

```
device# show ikev2 policy
```

```
Name : ike_policy_red
vrf : Default
Local address/Mask : 0.0.0.0/0.0.0.0
Proposal : ike_proposal_red
```

```
Name : ikev2-default-policy
vrf : Default
Proposal : ikev2-default-proposal
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ikev2 profile
Displays information about the configured IKEv2 profile.

Syntax
show ikev2 profile profile-name

Parameters
profile-name
Specifies the IKEv2 profile name.

Modes
Privileged EXEC mode

Examples
The following example displays show ikev2 profile command output.

device# show ikev2 profile
IKEv2 profile       : ike_profile_blue
Auth Profile        : auth_blue
Match criteria      :
IKE session vrf    : default-vrf
Local:              
    address 1.2.10.1
Remote:             
    address 1.2.10.2
Local identifier    : address 1.2.10.1
Remote identifier   : address 1.2.10.2
Local auth method: pki
Remote auth method(s): pki
Lifetime          : 86400 sec
keepalive check   : disabled

IKEv2 profile       : ike_profile_green
Auth Profile: auth_green
Match criteria:
IKE session vrf    : default-vrf
Local:              
    address 1.2.10.1
Remote:             
    address 1.2.10.2    fdqn RTB_green
Local identifier  : address 1.2.10.1
Remote identifier : address 1.2.10.2
Local auth method: pki
Remote auth method(s): pki
Lifetime          : 1440 minutes
keepalive check   : disabled

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ikev2 proposal
Displays configuration information about Internet Key Exchange version 2 (IKEv2) proposals.

Syntax
show ikev2 proposal [ name ]

Parameters
name
Specifies the name of an IKEv2 proposal.

Modes
User EXEC mode

Usage Guidelines
This command may be entered in all configuration modes.
When an IKEv2 proposal is not specified, this command displays configuration information for all IKEv2 proposals.

Command Output
The show ikev2 proposal command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of an IKEv2 proposal.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The encryption algorithms that are configured for the proposal.</td>
</tr>
<tr>
<td>Integrity</td>
<td>The integrity algorithms that are configured for the proposal.</td>
</tr>
<tr>
<td>PRF</td>
<td>The pseudorandom function algorithms that are configured for the proposal.</td>
</tr>
<tr>
<td>DH Group</td>
<td>The Diffie-Hellman groups that are configured for the proposal.</td>
</tr>
</tbody>
</table>

Examples
The following example shows how to display information about the IKEv2 proposal configuration.

device# show ikev2 proposal

Name : ikev2-default-proposal
Encryption : AES-CBC-256
Integrity : sha384
PRF : sha384
DH Group : 384_ECP/Group 20

History
Release version | Command history
--- | ---
5.8.00 | This command was introduced.
show ikev2 sa

Displays information about the current IKEv2 Security Associations (SA) that exist between the specified local and remote interfaces. This command supports IPsec IPv4 and IPv6.

Syntax

```
show ikev2 sa [spi-index | fvrf vrf-name | local [ address | ipv6-address ] | remote address ] [ detail ]
```

Parameters

- **spi-index**: (Optional) Specifies the IKEv2 Security Parameter Index (SPI) value.
- **fvrf vrf-name**: (Optional) Specifies the front VRF name.
- **local address**: (Optional) Specifies the IPv4 address of the local interface.
- **local ipv6-address**: (Optional) Specifies the IPv6 address of the local interface.
- **remote address**: (Optional) Specifies the IP address of the remote interface.
- **detail**: (Optional) Specifies to include details of the IKEv2 SA in the output.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not include the optional `detail` parameter, only the basic information about the SA is included in the output. If you want to view information about the interface role (initiator or responder), SPI indexes, or the selected IKEv2 policy or profile, make sure you include the `detail` parameter.

Examples

These examples are for IPsec IPv4.

The following example shows output for command `show ikev2 sa` for the SA between local interface 1.2.10.1 and remote interface 1.2.10.2. The `detail` keyword was not included.

```
device# show ikev2 sa

<table>
<thead>
<tr>
<th>tnl-id</th>
<th>local</th>
<th>remote</th>
<th>Status</th>
<th>vrf(i)</th>
<th>vrf(f)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tnl 2</td>
<td>1.2.10.1/500</td>
<td>1.2.10.2/500</td>
<td>rdy</td>
<td>Blue</td>
<td>Default</td>
</tr>
</tbody>
</table>
```
The following example shows output for command `show ikev2 sa detail` for the SA between local interface 1.2.10.1 and remote interface 1.2.10.2. The `detail` keyword was included.

```
device# show ikev2 sa detail

<table>
<thead>
<tr>
<th>tnl-id</th>
<th>local</th>
<th>remote</th>
<th>status</th>
<th>vrf(l)</th>
<th>vrf(f)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.2.10.1/500</td>
<td>1.2.10.2/500</td>
<td>rdy</td>
<td>Blue</td>
<td>Default</td>
</tr>
</tbody>
</table>

Role: Initiator
Local SPI: 0xf327d32cd0df9106 Remote SPI: 0x34bec986ed6c232e
Ike Profile: mlx2_1
Ike Policy: mlx2_1
Auth Proposal: def-Ike-auth-prop
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.9.00</td>
<td>This command was modified to add support for IPsec IPv6.</td>
</tr>
</tbody>
</table>
show ikev2 session

Displays information about the configured IKEv2 profile.

Syntax

```
show ikev2 session [local-spi-id] [detail]
```

Parameters

`local-spi-id`

Specifies the local SPI ID value.

`detail`

Specifies the detailed description of the IKEv2 profile.

Modes

Privileged EXEC mode

Examples

The following example displays `show ikev2 session` command output.

```
device# show ikev2 session
IKE count:1, CHILD count:1
Tunnel-id Local Remote Status vrf(i) vrf(f)
--------------------------------------------------------
Tnl 2 1.2.10.1/500 1.2.10.2/500 rdy|in-use Blue Default
child sa:
id 1
  local selector 0.0.0.0/0 - 255.255.255.255/65535
  remote selector 0.0.0.0/0 - 255.255.255.255/65535
  ESP spi in/out: 0x0000004b/0x0000005e
  Encryption: aes-gcm-256, ICV Size: 16 octects, Esp_hmac: null
  Authentication: null  DH Group:none , Mode: tunnel
```
The following example displays `show ikev2 session detailed` command output.

device# show ikev2 session detailed

IKE count:1, CHILD count:1

<table>
<thead>
<tr>
<th>Tunnel-id</th>
<th>Local</th>
<th>Remote</th>
<th>Status</th>
<th>vrf(p)</th>
<th>vrf(f)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.2.10.1/500</td>
<td>1.2.10.2/500</td>
<td>rdy</td>
<td>in-use Blue Default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Life/Active Time: 86400/361 sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Status Description: Negotiation done</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local spi: f7c029048eb25082</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remote spi: 56b8735e2f6afbd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local id : address 1.2.45.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remote id : address 1.2.45.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No Exchange in Progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next Request Message id=29</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Keepalive sent: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Keepalive Received: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time Past Since Last Msg: 60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

child sa:
id 1

| local selector  | 0.0.0.0/0 - 255.255.255.255/65535 |
| remote selector | 0.0.0.0/0 - 255.255.255.255/65535 |
| ESP spi in/out  | 0x00000004b/0x00000005e |
| Encryption      | aes-gcm-256, ICV Size: 16 octects, Esp_hmac: null |
| Authentication  | null DH Group:none , Mode: tunnel |

---

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ikev2 statistics

Displays statistical information about Internet Key Exchange version 2 (IKEv2).

Syntax

show ikev2 statistics

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

Command Output

The `show ikev2 statistics` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total IKEv2 SA Count active</td>
<td>The total number of IKEv2 security associations (SAs) in an active state.</td>
</tr>
<tr>
<td>Incoming IKEv2 Requests</td>
<td>The number of IKEv2 SAs (accepted and rejected) initiated by the peer device.</td>
</tr>
<tr>
<td>Outgoing IKEv2 Requests</td>
<td>The number of IKEv2 SAs initiated by the local device.</td>
</tr>
<tr>
<td>Accepted</td>
<td>The total number of outgoing IKEv2 SAs that were accepted.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The total number of outgoing IKEv2 SAs that were rejected.</td>
</tr>
<tr>
<td>Rejected due to no cookie</td>
<td>The total number of outgoing IKEv2 SAs that were rejected due to no cookie.</td>
</tr>
<tr>
<td>IKEv2 Packet Statistics</td>
<td></td>
</tr>
<tr>
<td>Total Packets Received</td>
<td>The total number of packets received.</td>
</tr>
<tr>
<td>Total Packets Transmitted</td>
<td>The total number of packets transmitted.</td>
</tr>
<tr>
<td>Total Packets Retransmitted</td>
<td>The total number of packets retransmitted.</td>
</tr>
<tr>
<td>Total Failed Transmission</td>
<td>The total number of packets where transmission failed.</td>
</tr>
<tr>
<td>Total Pending Packets</td>
<td>The total number of packets to be transmitted.</td>
</tr>
<tr>
<td>Total Buffer Failed</td>
<td>The total number of packets where transmission failed due to a buffer issue.</td>
</tr>
<tr>
<td>Total Keepalive Received</td>
<td>The total number of IKEv2 keepalive messages received.</td>
</tr>
<tr>
<td>Total Keepalive Transmitted</td>
<td>The total number of IKEv2 keepalive messages transmitted.</td>
</tr>
<tr>
<td>IKEv2 Error Statistics</td>
<td></td>
</tr>
<tr>
<td>Unsupported Payload</td>
<td>The total number of IKEv2 packets received with an unsupported payload.</td>
</tr>
<tr>
<td>Invalid IKE SPI</td>
<td>The total number of IKEv2 packets received with an invalid security parameter index (SPI).</td>
</tr>
<tr>
<td>Invalid Version</td>
<td>The total number of IKEv2 packets received with an invalid version.</td>
</tr>
<tr>
<td>Invalid Syntax</td>
<td>The total number of IKEv2 packets received with invalid syntax.</td>
</tr>
<tr>
<td>Negotiation Timeout</td>
<td>The total number of IKEv2 sessions deleted due to dead peer detection (DPD) or negotiation timeouts.</td>
</tr>
<tr>
<td>No Policy</td>
<td>The total number of IKEv2 sessions deleted or rejected due to a policy issue.</td>
</tr>
<tr>
<td>No Protection Suite</td>
<td>The total number of IKEv2 sessions deleted or rejected due to a protection suite issue.</td>
</tr>
<tr>
<td>Policy Error</td>
<td>The total number of IKEv2 sessions deleted or rejected due to policy error.</td>
</tr>
</tbody>
</table>
### Output field Description

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Packet Error</td>
<td>The total number of IKEv2 or IPsec packets received with a packet error.</td>
</tr>
<tr>
<td>Discard Policy</td>
<td>The total number of IKEv2 or IPsec sessions deleted or rejected due to a policy error or mismatch.</td>
</tr>
<tr>
<td>Proposal Mismatch</td>
<td>The total number of IKEv2 or IPsec packets sent or received with a proposal mismatch.</td>
</tr>
<tr>
<td>Invalid Selectors</td>
<td>The total number of IKEv2 or IPsec packets sent or received with invalid selectors.</td>
</tr>
<tr>
<td>Internal Error</td>
<td>The total number of IKEv2 or IPsec packets sent or received with an internal error.</td>
</tr>
<tr>
<td>SA Overflow</td>
<td>The total number of times the maximum SA count was reached.</td>
</tr>
<tr>
<td>IKE SA Overflow</td>
<td>The number of times the maximum IKEv2 SA count was reached.</td>
</tr>
<tr>
<td>IPSEC SA Overflow</td>
<td>The number of times the maximum IPsec SA count was reached.</td>
</tr>
<tr>
<td>Authentication Failed</td>
<td>The total number of IKEv2 or IPsec packets sent or received when authentication failed.</td>
</tr>
<tr>
<td>Others</td>
<td>The total number of IKEv2 or IPsec packets sent or received with other error types.</td>
</tr>
<tr>
<td>Number of HW-SPI Add write</td>
<td>The number of times the creation of an IPsec SPI was written to the hardware.</td>
</tr>
<tr>
<td>Number of HW-SPI Delete</td>
<td>The number of times the deletion of an IPsec SPI was written to the hardware.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays `show ikev2 statistics` command output.

```
device#show ikev2 statistics
Total IKEv2 SA Count : 1 active: 1 negotiating: 0
Incoming IKEv2 Requests: 0 accepted: 0 rejected: 0
Outgoing IKEv2 Requests: 1 accepted: 1 rejected: 0
Rejected IKEv2 Requests: 0
Incoming IKEV2 Cookie Challenged Requests: 0 accepted: 0 rejected: 0 rejected no cookie: 0
IKEv2 Packet Statistics:
    Total Packets Received : 57
    Total Packets Transmitted: 57
    Total Packets Retransmitted: 0
    Total Keepalive Received : 10
    Total Keepalive Transmitted: 10
IKEv2 Error Statistics:
    Unsupported Payload : 0 Invalid IKE SPI : 0
    Invalid Version : 0 Invalid Syntax : 0
    Proposal Mismatch : 0 Invalid Selectors: 0
    Authentication Failed : 0 Others : 0
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00a</td>
<td>This command was modified to include output fields for extended IKEv2 counters.</td>
</tr>
</tbody>
</table>
**show interface ethernet**

Displays the interfaces associated with the specified port.

**Syntax**

```
show interface ethernet <slot/port>
```

**Parameters**

- **slot/port**
  
  Indicate the slot and port for the port of which the interface information is required.

**Modes**

This command operates under all modes.

**Command Output**

The `show interface ethernet` command displays the following information in list form.

**Examples**

```bash
Brocade(config)#show interface ethernet 1/1
10GigabitEthernet5/1 is disabled, line protocol is down
  STP Root Guard is disabled, STP BPDU Guard is disabled
  Hardware is 10GigabitEthernet, address is 001b.edae.6e00 (bia 001b.edae.6ec0)
  Configured speed 10Gbit, actual unknown, configured duplex fdx, actual unknown
  Member of Control VLAN 4095, VLAN 1 (untagged), 1 L2 VLANS (tagged),
  port is in dual mode (default vlan), port state is Disabled
  STP configured to ON, Priority is level0, flow control enabled
  Egress truncate is ON, egress truncate size is 64 bytes
  Priority force disabled, Drop precedence level 0, Drop precedence force disabled
  dhcp-snooping-trust configured to OFF
  mirror disabled, monitor disabled
  LACP BPDU Forwarding:Disabled
  LLDP BPDU Forwarding:Disabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  Port is not enabled to receive all vlan packets for pbr
  MTU 1548 bytes, encapsulation ethernet
  Openflow: Disabled, Openflow Index 193
  Cluster L2 protocol forwarding enabled
  300 second input rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  300 second output rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts, 0 unicasts
  0 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  NP received 0 packets, Sent to TM 0 packets
  NP Ingress dropped 0 packets
  0 packets output, 0 bytes, 0 underruns
  Transmitted 0 broadcasts, 0 multicasts, 0 unicasts
  0 output errors, 0 collisions
  NP transmitted 0 packets, Received from TM 0 packets
```
The following example shows an output with the port-state-change time highlighted for port 3 on slot 1.

```
Brocade(config)#show interface ethernet 1/3
10GigabitEthernet1/3 is up, line protocol is down (LACP-BLOCKED)
  Port state change time: Jan 21 02:40:21, (0 days, 00:07:16 ago)
  Loopback: None
  STP Root Guard is disabled, STP BPDU Guard is disabled
  Hardware is 10GigabitEthernet, address is 0024.38a4.3802 (bia 0024.38a4.3802)
  ... NP transmitted 11115 packets, Received from TM 11115 packets
```

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to display Egress truncate status and configured size and port state change time.</td>
</tr>
</tbody>
</table>
show interfaces tunnel

Displays the IP addresses and unicast and multicast traffic counters for the specified IPv4 IPsec tunnel. This command cannot be used on IPv6 IPsec tunnels.

Syntax

```
show interfaces tunnel num
```

Parameters

`num`

Specifies the tunnel number.

Modes

User EXEC mode

Command Output

The `show interfaces tunnel` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel number</td>
<td>The number of the tunnel.</td>
</tr>
<tr>
<td>Tunnel source</td>
<td>The IP address of the interface that is configured as the source of the tunnel. IP packets are forwarded from this interface across the tunnel.</td>
</tr>
<tr>
<td>Tunnel destination</td>
<td>The IP address of the interface that is configured as the destination of the tunnel. IP packets forwarded from the tunnel source interface are received by this interface.</td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>The specified tunnel mode for the tunnel. This indicates which version of IP (IPv4 or IPv6) has been enabled on the tunnel interface.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>The tunnel mode is always IPv4 when using this command (this command can only be used on IPv4 IPsec tunnels).</td>
</tr>
<tr>
<td>Port name</td>
<td>The specified name of the port. If a name was not specified, the output shows no port name.</td>
</tr>
<tr>
<td>Internet address</td>
<td>The IP address of the port. This is not the IP address of the tunnel source or destination.</td>
</tr>
<tr>
<td>Tunnel TOS</td>
<td>The value to write into the ToS byte in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 99, where 0 means a tunnel packet copies the ToS value from the packet being encapsulated (the passenger packet).</td>
</tr>
<tr>
<td>Tunnel TTL</td>
<td>The value to write into the TTL field in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 255, where 0 means a tunnel packet copies the value from the packet being encapsulated (the passenger packet). The default value is 255.</td>
</tr>
<tr>
<td>Tunnel MTU</td>
<td>This maximum size allowable for IP packets entering the tunnel. Packets that exceed the value you specify (or the default) are sent back to the source. The default value is 1480 bytes.</td>
</tr>
<tr>
<td>Tunnel vrf</td>
<td></td>
</tr>
<tr>
<td>Forwarding vrf</td>
<td></td>
</tr>
<tr>
<td>Tunnel protection profile</td>
<td>The name of the IPsec profile used to encapsulate and encrypt the IP packets being transmitted by the tunnel interface. A tunnel profile defines a set of encapsulation and encryption methods used to secure IP packets.</td>
</tr>
<tr>
<td>Tunnel packet statistics</td>
<td>The following packet counts for unicast traffic on the tunnel.</td>
</tr>
</tbody>
</table>
### Output field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxPkts: The total number of IP packets received from the tunnel on the interface.</td>
</tr>
<tr>
<td>TxPkts: The total number of IP packets transmitted across the tunnel from the interface.</td>
</tr>
<tr>
<td>RxBytes: The total number of bytes received from the tunnel on the interface. (The total is for IP packets only.)</td>
</tr>
<tr>
<td>TxBytes: The total number of bytes transmitted across the tunnel from the interface. (The total is for IP packets only.)</td>
</tr>
</tbody>
</table>

### Tunnel multicast packet statistics

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following packet counts for multicast traffic on the tunnel:</td>
</tr>
<tr>
<td>RxMcPkts: The total number of IP multicast packets received from the tunnel on the interface.</td>
</tr>
<tr>
<td>TxMcPkts: The total number of IP multicast packets transmitted across the tunnel from the interface.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is restricted to showing data for IPv4 IPsec tunnels.

**NOTE**

If you want to view the same information for IPv6 IPsec tunnels, use the `show ipv6 interface tunnel` command.

### Examples

The following example shows output for tunnel number 10.

```bash
device# show interfaces tunnel 10
Tunnel10 is IPSec port up, line protocol is up
    Hardware is Tunnel
    Tunnel source is 1.1.1.1
    Tunnel destination is 1.1.1.2
    Tunnel mode IPSec IPv4
    No port name
    Internet address is: 11.11.11.5/24
    Tunnel TOS 0, Tunnel TTL 255, Tunnel MTU 1431 bytes
    Tunnel vrf (IVRF): default-vrf
    Forwarding vrf(FVRF): default-vrf
    Tunnel protection profile: abcd
    Tunnel Packet Statistics:
        RxPkts: 100          TxPkts: 11200
        RxBytes: 150         TxBytes: 12544
    Tunnel Multicast Packet Statistics:
        RxMcPkts: 5394      TxMcPkts:  67
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include multicast packet statistics information for the tunnel.</td>
</tr>
</tbody>
</table>
show ip allow-src-multicast
Displays whether the packet drop for multicast IPv4 or IPv6 as the source IP address is enabled or disabled.

Syntax
```
show ip allow-src-multicast [switched-only]
```

Parameters
- **switched-only**
  Displays switched multicast traffic as the source IP address.

Modes
User EXEC mode

Command Output
The `show ip allow-src-multicast` command displays the following information.

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable packet drop for multicast IPv4/IPv6 as source IP</td>
<td>Displays whether the disable packet drop for multicast IPv4 or IPv6 addresses as the source IP address is enabled or disabled.</td>
</tr>
<tr>
<td>Disable packet drop for multicast switched traffic only</td>
<td>Displays the slot on which the disable packet drop for switched traffic only is enabled.</td>
</tr>
</tbody>
</table>

Examples
The following example displays the disable packet drop for multicast IPv4 or IPv6 addresses as source IP address in a disabled state.
```
device# show ip allow-src-multicast
Disable packet drop for multicast ipv4/ipv6 as source ip:
DISABLED
```

The following example displays the disabled packet drop for switched traffic only in an enabled state for slot 3.
```
device# show ip allow-src-multicast switched-only
Disable packet drop for switched traffic only:
ENABLED ON:
Slot 3
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ip bgp

Displays entries in the IPv4 Border Gateway Protocol (BGP4) routing table.

Syntax

show ip bgp
show ip bgp ip-addr [ /prefix ]
show ip bgp ip-addr [ /prefix ] longer-prefixes

Parameters

ipv6-addr/prefix
IPv4 address and optional prefix.

longer-prefixes
Filters on prefixes equal to or greater than that specified by prefix.

Modes

User EXEC mode

Examples

This example displays sample output from the show ip bgp command.

device# show ip bgp

Total number of BGP Routes: 4
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop MED LocPrf Weight Path
*>i 110.110.110.0/24 50.50.50.10 150 0 1
*x 110.110.110.0/24 20.20.20.10 100 0 200 i
*x 110.110.110.0/24 30.30.30.10 100 0 300 i
*x 110.110.110.0/24 40.40.40.10 100 0 400 i

This example displays sample output from the show ip bgp command when an IP address is specified.

device# show ip bgp 10.3.4.0

Number of BGP Routes matching display condition: 1
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 10.3.4.0/24 192.168.4.106 100 0 65001 4355 1 1221 ?

Last update to IP routing table: 0h11m38s, 1 path(s) installed:
Gateway Port
192.168.2.1 2/1
Route is advertised to 1 peers:
10.20.20.2(65300)
show ip bgp attribute-entries

Displays BGP4 route-attribute entries that are stored in device memory.

Syntax

show ip bgp attribute-entries

Modes

User EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4 attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4 route-attribute entries that are stored in device memory.

Command Output

The `show ip bgp attribute-entries` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of BGP4 Attribute Entries</td>
<td>The number of routes contained in this BGP4 route table.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The IP address of the next-hop device for routes that have this set of attributes.</td>
</tr>
<tr>
<td>Metric</td>
<td>The cost of the routes that have this set of attributes.</td>
</tr>
<tr>
<td>Origin</td>
<td>The source of the route information. The origin can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• EGP - The routes with these attributes came to BGP4 through EGP.</td>
</tr>
<tr>
<td></td>
<td>• IGP - The routes with these attributes came to BGP4 through IGP.</td>
</tr>
<tr>
<td></td>
<td>• INCOMPLETE - The routes came from an origin other than one of the above. For example, they may have been redistributed from OSPF or RIP.</td>
</tr>
<tr>
<td></td>
<td>When BGP4 compares multiple routes to a destination to select the best route, IGP is preferred over EGP and both are preferred over INCOMPLETE.</td>
</tr>
<tr>
<td>Originator</td>
<td>The originator of the route in a route reflector environment.</td>
</tr>
<tr>
<td>Cluster List</td>
<td>The route-reflector clusters through which this set of attributes has passed.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>Aggregator information:</td>
</tr>
<tr>
<td></td>
<td>• AS Number shows the AS in which the network information in the attribute set was aggregated. This value applies only to aggregated routes and is otherwise 0.</td>
</tr>
<tr>
<td></td>
<td>• Router-ID shows the device that originated this aggregator.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Atomic       | Whether the network information in this set of attributes has been aggregated and this aggregation has resulted in information loss.  
  - TRUE - Indicates information loss has occurred  
  - FALSE - Indicates no information loss has occurred  

**NOTE**  
Information loss under these circumstances is a normal part of BGP4 and does not indicate an error. |
| Local Pref   | The degree of preference for routes that use these attributes relative to other routes in the local AS. |
| Communities  | The communities to which routes with these attributes belong. |
| AS Path      | The autonomous systems through which routes with these attributes have passed. The local AS is shown in parentheses. |

**Examples**

The following example show sample output for the `show ip bgp attribute-entries` command.

```
device# show ip bgp attribute-entries

  Total number of BGP Attribute Entries: 18 (0)

  1       Next Hop  :192.168.1.6        MED :1             Origin:INCOMP
          Originator:0.0.0.0            Cluster List:None
          Aggregator:AS Number :0       Router-ID:0.0.0.0      Atomic:None
          Local Pref:100               Communities:Internet
          Extended Community: SOO 300000:3
          AS Path   :90000 80000 (length 11)
          Address: 0x10e4e0c4  Hash:489 (0x03028536), PeerIdx 0
          Links: 0x0000000000, 0x0000000000, nri: 0x10f4804a
          Reference Counts: 1:0:1, Magic: 51

  2       Next Hop  :192.168.1.5        Metric :1          Origin:INCOMP
          Originator:0.0.0.0            Cluster List:None
          Aggregator:AS Number :0       Router-ID:0.0.0.0      Atomic:None
          Local Pref:100               Communities:Internet
          Extended Community: RT 200000:12
          AS Path   :900000 75000 (length 11)
          Address: 0x10e4e062  Hash:545 (0x0301e8f6), PeerIdx 0
          Links: 0x0000000000, 0x0000000000, nri: 0x10f47ff0
          Reference Counts: 1:0:1, Magic: 49
```
show ip bgp config

Displays active BGP4 configuration information.

Syntax

  show ip bgp config

Modes

  User EXEC mode

Examples

This example displays sample output from the show ip bgp config command.

device# show ip bgp config

router bgp
  local-as 200
  neighbor 10.102.1.1 remote-as 200
  neighbor 10.102.1.1 ebgp-multihop
  neighbor 10.102.1.1 update-source loopback 1
  neighbor 192.168.2.1 remote-as 100
  neighbor 10.200.2.2 remote-as 400
  neighbor 2001:db8::1:1 remote-as 200
  neighbor 2001:db8::1:2 remote-as 400
  neighbor 2001:db8::1 remote-as 300

  address-family ipv4 unicast
  no neighbor 2001:db8::1:1 activate
  no neighbor 2001:db8::1:2 activate
  no neighbor 2001:db8::1 activate
  exit-address-family

  address-family ipv4 multicast
  exit-address-family

  address-family ipv6 unicast
  redistribute static
  neighbor 2001:db8::1:1 activate
  neighbor 2001:db8::1:2 activate
  neighbor 2001:db8::1 activate
  exit-address-family

  end of BGP configuration
show ip bgp dampened-paths

Displays all BGP4 dampened routes.

Syntax

  show ip bgp dampened-paths

Modes

  User EXEC mode
show ip bgp filtered-routes
Displays BGP4 filtered routes that are received from a neighbor or peer group.

Syntax

```
show ip bgp filtered-routes [ detail ] [ ip-addr { / mask } [ longer-prefixes ] ] | as-path-access-list name ] | prefix-list name ]
```

Parameters

detail
Optionally displays detailed route information.

ip-addr
IPv4 address of the destination network in dotted-decimal notation.

mask
(Optional) IPv4 mask of the destination network in CIDR notation.

longer-prefixes
Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

as-path-access-list name
Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

prefix-list name
Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

name
Name of an AS-path ACL or prefix list.

Modes
User EXEC mode

Examples

This example displays BGP4 filtered routes.

```
device# show ip bgp filtered-routes
Searching for matching routes, use ^C to quit...
Prefix           Next Hop          MED     LocPrf     Weight Status
1    10.3.0.0/8          192.168.4.106              100        0      EF
   AS_PATH: 65001 4355 701 80
2    10.4.0.0/8          192.168.4.106              100        0      EF
   AS_PATH: 65001 4355 1
3    10.60.212.0/22      192.168.4.106              100        0      EF
   AS_PATH: 65001 4355 701 1 189
```
show ip bgp flap-statistics
Displays BGP4 route-dampening statistics for all dampened routes with a variety of options.

Syntax

```
show ip bgp flap-statistics
show ip bgp flap-statistics ip-addr { / mask } { longer-prefix }
show ip bgp flap-statistics as-path-filter name
show ip bgp flap-statistics neighbor ip-addr
show ip bgp flap-statistics regular-expression name
```

Parameters

- **ip-addr**
  IPv4 address of a specified route in dotted-decimal notation.
- **mask**
  IPv4 mask of a specified route in CIDR notation.
- **longer-prefixes**
  Displays statistics for routes that match the specified route or have a longer prefix than the specified route.
- **as-path-filter name**
  Specifies an AS-path filter.
- **neighbor**
  Displays flap statistics only for routes learned from the specified neighbor.
  
  - **ip-addr**
    IPv4 address of the neighbor.
- **regular-expression**
  Specifies a regular expression in the display output on which to filter.
  
  - **name**
    Name of an AS-path filter or regular expression.

Modes

- User EXEC mode

Command Output

The `show ip bgp flap-statistics` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of flapping routes</td>
<td>The total number of routes in the BGP4 route table that have changed state and have been marked as flapping routes.</td>
</tr>
<tr>
<td>Status code</td>
<td>Indicates the dampening status of the route, which can be one of the following:</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>&gt;</td>
<td>This is the best route among those in the BGP4 route table to the route destination.</td>
</tr>
<tr>
<td>d</td>
<td>This route is currently dampened, and unusable.</td>
</tr>
<tr>
<td>h</td>
<td>The route has a history of flapping and is unreachable now.</td>
</tr>
<tr>
<td>*</td>
<td>The route has a history of flapping but is currently usable.</td>
</tr>
</tbody>
</table>

Network | The destination network of the route.

From | The neighbor that sent the route to the device.

Flaps | The number of flaps the route has experienced.

Since | The amount of time since the first flap of this route.

Reuse | The amount of time remaining until this route will be un-suppressed and can be used again.

Path | Shows the AS-path information for the route.

Examples
The following example displays route dampening statistics.

device# show ip bgp flap-statistics
Total number of flapping routes: 414

<table>
<thead>
<tr>
<th>Network</th>
<th>From</th>
<th>Flaps</th>
<th>Since</th>
<th>Reuse</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>h&gt; 10.50.206.0/23</td>
<td>10.90.213.77</td>
<td>1</td>
<td>0:0:13</td>
<td>0:0:0</td>
<td>65001 4355 1 701</td>
</tr>
<tr>
<td>h&gt; 10.255.192.0/20</td>
<td>10.90.213.77</td>
<td>1</td>
<td>0:0:13</td>
<td>0:0:0</td>
<td>65001 4355 1 7018</td>
</tr>
<tr>
<td>h&gt; 10.252.165.0/24</td>
<td>10.90.213.77</td>
<td>1</td>
<td>0:0:13</td>
<td>0:0:0</td>
<td>65001 4355 1 7018</td>
</tr>
<tr>
<td>h&gt; 10.50.208.0/23</td>
<td>10.90.213.77</td>
<td>1</td>
<td>0:0:13</td>
<td>0:0:0</td>
<td>65001 4355 1 701</td>
</tr>
<tr>
<td>h&gt; 10.33.0.0/16</td>
<td>10.90.213.77</td>
<td>1</td>
<td>0:0:13</td>
<td>0:0:0</td>
<td>65001 4355 1 701</td>
</tr>
<tr>
<td>* &gt; 10.17.220.0/24</td>
<td>10.90.213.77</td>
<td>1</td>
<td>0:1:4</td>
<td>0:0:0</td>
<td>65001 4355 701 62</td>
</tr>
</tbody>
</table>
show ip bgp ipv6

Displays IPv6 unicast information.

Syntax

show ip bgp ipv6 neighbors

show ip bgp ipv6 neighbors ip-addr advertised-routes [ detail ] [ ipv6 address /mask ]

show ip bgp ipv6 neighbors ip-addr flap-statistics

show ip bgp ipv6 neighbors ip-addr last-packet-with-error [ decode ]

show ip bgp ipv6 neighbors ip-addr received [ prefix-filter ]

show ip bgp ipv6 neighbors ip-addr received-routes [ detail ]

show ip bgp ipv6 neighbors ip-addr rib-out-routes [ detail ] [ ipv6 address /mask ]

show ip bgp ipv6 neighbors ip-addr routes

show ip bgp ipv6 neighbors ip-addr routes { best | not-installed-best | unreachable }

show ip bgp ipv6 neighbors ip-addr routes detail { best | not-installed-best | unreachable }

show ip bgp ipv6 neighbors ip-addr routes-summary

show ip bgp ipv6 neighbors last-packet-with-error

show ip bgp ipv6 neighbors routes-summary

show ip bgp ipv6 summary

Parameters

neighbors

Specifies a neighbor.

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

advertised-routes

Specifies the routes that the device has advertised to the neighbor during the current BGP4 session.

detail

Specifies detailed information.

ipv6 address /mask

Specifies an IPv6 address and mask.

flap-statistics

Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

last-packet-with-error

Specifies the last packet with an error.

decode

Decodes the last packet that contained an error from any of a device’s neighbors.
received
  Specifies Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

prefix-filter
  Displays the results for ORFs that are prefix-based.

received-routes
  Specifies all route information received in route updates from BGP4 neighbors of the device since the soft-
  reconfiguration feature was enabled.

rib-out-routes
  Displays information about the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and
  specific destination networks.

routes
  Displays a variety of route information received in UPDATE messages from BGP4 neighbors.

best
  Displays routes received from the neighbor that are the best BGP4 routes to their destination.

not-installed-best
  Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in
  the route table because the device received better routes from other sources.

unreachable
  Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next
  hop.

routes-summary
  Displays all route information received in UPDATE messages from BGP4 neighbors.

summary
  Displays summarized IPv6 unicast information.

Modes
User EXEC mode

Examples
The following example displays summarized IPv6 unicast information.

device> show ip bgp ipv6 summary
BGP4 Summary
  Router ID: 10.1.1.1 Local AS Number: 1
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 1, UP: 1
  Number of Routes Installed: 1, Uses 86 bytes
  Number of Routes Advertising to All Neighbors: 0 (0 entries)
  Number of Attribute Entries Installed: 1, Uses 90 bytes
  Neighbor Address AS# State Time Rt:Accepted Filtered Sent ToSend
  192.168.1.2 2 ESTAB 0h 1m 51s 1 0 0 0
The following example displays IPv6 unicast device information with respect to IPv4 neighbors.

device(config-bgp)# show ip bgp ipv6 neighbors
Total number of BGP Neighbors: 1
1 IP Address: 192.168.1.2, AS: 2 (EBGP), RouterID: 10.1.1.2, VRF: default-vrf
State: ESTABLISHED, Time: 0h8m33s, KeepAliveTime: 60, HoldTime: 180
KeepAliveTimer Expire in 17 seconds, HoldTimer Expire in 135 seconds
UpdateSource: Loopback 1
RefreshCapability: Received
....... Neighbor NLRI Negotiation:
Peer Negotiated IPV6 unicast capability
Peer configured for IPV6 unicast Routes
Neighbor ipv6 MPLS Label Capability Negotiation:
Neighbor AS4 Capability Negotiation:
TCP Connection state: ESTABLISHED, flags:00000033 (0,0)
**show ip bgp neighbors**

Displays configuration information and statistics for BGP4 neighbors of the device.

**Syntax**

```
show ip bgp neighbors [ip-addr]
show ip bgp neighbors last-packet-with-error
show ip bgp neighbors routes-summary
```

**Parameters**

- **ip-addr**
  IPv4 address of a neighbor in dotted-decimal notation.

- **last-packet-with-error**
  Displays the last packet with an error.

- **routes-summary**
  Displays routes received, routes accepted, number of routes advertised by peer, and so on.

**Modes**

User EXEC mode

**Usage Guidelines**

Use this command to view configuration information and statistics for BGP neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

**Command Output**

The **show ip bgp neighbors** command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of BGP4 Neighbors</td>
<td>The number of BGP4 neighbors configured.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the neighbor.</td>
</tr>
<tr>
<td>AS</td>
<td>The AS the neighbor is in.</td>
</tr>
<tr>
<td>EBGp or IBGP</td>
<td>Whether the neighbor session is an IBGP session, an EBGp session, or a</td>
</tr>
<tr>
<td></td>
<td>confederation EBGp session:</td>
</tr>
<tr>
<td></td>
<td>• EBGp - The neighbor is in another AS.</td>
</tr>
<tr>
<td></td>
<td>• EBGp_Conf - The neighbor is a member of another sub-AS in the same</td>
</tr>
<tr>
<td></td>
<td>sub-AS in the same confederation.</td>
</tr>
<tr>
<td></td>
<td>• IBGP - The neighbor is in the same AS.</td>
</tr>
<tr>
<td>RouterID</td>
<td>The neighbor device ID.</td>
</tr>
<tr>
<td>Description</td>
<td>The description you gave the neighbor when you configured it on the device.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The value (if any) of the Local AS configured.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The state of the session with the neighbor. The states are from the device perspective, not the neighbor perspective. The state values are based on the BGP4 state machine values described in RFC 1771 and can be one of the following for each device:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- CONNECT - BGP4 is waiting for the connection process for the TCP neighbor session to be completed.</td>
</tr>
<tr>
<td></td>
<td>- ACTIVE - BGP4 is waiting for a TCP connection from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>NOTE If the state frequently changes between CONNECT and ACTIVE, there may be a problem with the TCP connection.</td>
</tr>
<tr>
<td></td>
<td>- OPEN SENT - BGP4 is waiting for an Open message from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- ESTABLISHED - BGP4 is ready to exchange UPDATE messages with the neighbor.</td>
</tr>
<tr>
<td>Time</td>
<td>The amount of time this session has been in the current state.</td>
</tr>
<tr>
<td>KeepAliveTime</td>
<td>The keep alive time, which specifies how often this device sends keepalive messages to the neighbor.</td>
</tr>
<tr>
<td>HoldTime</td>
<td>The hold time, which specifies how many seconds the device will wait for a keepalive or update message from a BGP4 neighbor before deciding that the neighbor is not operational.</td>
</tr>
<tr>
<td>PeerGroup</td>
<td>The name of the peer group the neighbor is in, if applicable.</td>
</tr>
<tr>
<td>Multihop-EBGP</td>
<td>Whether this option is enabled for the neighbor.</td>
</tr>
<tr>
<td>RouteReflectorClient</td>
<td>Whether this option is enabled for the neighbor.</td>
</tr>
<tr>
<td>SendCommunity</td>
<td>Whether this option is enabled for the neighbor.</td>
</tr>
<tr>
<td>NextHopSelf</td>
<td>Whether this option is enabled for the neighbor.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DefaultOriginate</td>
<td>Whether this option is enabled for the neighbor.</td>
</tr>
<tr>
<td>MaximumPrefixLimit</td>
<td>Maximum number of prefixes the device will accept from this neighbor.</td>
</tr>
<tr>
<td>RemovePrivateAs</td>
<td>Whether this option is enabled for the neighbor.</td>
</tr>
<tr>
<td>RefreshCapability</td>
<td>Whether this device has received confirmation from the neighbor that the neighbor supports the dynamic refresh capability.</td>
</tr>
<tr>
<td>CooperativeFilteringCapability</td>
<td>Whether the neighbor is enabled for cooperative route filtering.</td>
</tr>
<tr>
<td>Distribute-list</td>
<td>Lists the distribute list parameters, if configured.</td>
</tr>
<tr>
<td>Filter-list</td>
<td>Lists the filter list parameters, if configured.</td>
</tr>
<tr>
<td>Prefix-list</td>
<td>Lists the prefix list parameters, if configured.</td>
</tr>
<tr>
<td>Route-map</td>
<td>Lists the route map parameters, if configured.</td>
</tr>
<tr>
<td>Messages Sent</td>
<td>The number of messages this device has sent to the neighbor. The display shows statistics for the following message types:</td>
</tr>
<tr>
<td></td>
<td>- Open</td>
</tr>
<tr>
<td></td>
<td>- Update</td>
</tr>
<tr>
<td></td>
<td>- KeepAlive</td>
</tr>
<tr>
<td></td>
<td>- Notification</td>
</tr>
<tr>
<td></td>
<td>- Refresh-Req</td>
</tr>
<tr>
<td>Messages Received</td>
<td>The number of messages this device has received from the neighbor. The message types are the same as for the Message Sent field.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>Lists the last time updates were sent and received for the following:</td>
</tr>
<tr>
<td></td>
<td>- NLRIs</td>
</tr>
<tr>
<td></td>
<td>- Withdraws</td>
</tr>
<tr>
<td>Last Connection Reset Reason</td>
<td>The reason the previous session with this neighbor ended. The reason can be one of the following: Reasons described in the BGP4 specifications:</td>
</tr>
<tr>
<td></td>
<td>- Message Header Error</td>
</tr>
<tr>
<td></td>
<td>- Connection Not Synchronized</td>
</tr>
<tr>
<td></td>
<td>- Bad Message Length</td>
</tr>
<tr>
<td></td>
<td>- Bad Message Type</td>
</tr>
<tr>
<td></td>
<td>- OPEN Message Error</td>
</tr>
<tr>
<td></td>
<td>- Unsupported Version Number</td>
</tr>
<tr>
<td></td>
<td>- Bad Peer AS Number</td>
</tr>
<tr>
<td></td>
<td>- Bad BGP4 Identifier</td>
</tr>
<tr>
<td></td>
<td>- Unsupported Optional Parameter</td>
</tr>
<tr>
<td></td>
<td>- Authentication Failure</td>
</tr>
<tr>
<td></td>
<td>- Unacceptable Hold Time</td>
</tr>
<tr>
<td></td>
<td>- Unsupported Capability</td>
</tr>
<tr>
<td></td>
<td>- UPDATE Message Error</td>
</tr>
<tr>
<td></td>
<td>- Malformed Attribute List</td>
</tr>
<tr>
<td></td>
<td>- Unrecognized Well-known Attribute</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Missing Well-known Attribute</td>
</tr>
<tr>
<td></td>
<td>• Attribute Flags Error</td>
</tr>
<tr>
<td></td>
<td>• Attribute Length Error</td>
</tr>
<tr>
<td></td>
<td>• Invalid ORIGIN Attribute</td>
</tr>
<tr>
<td></td>
<td>• Invalid NEXT_HOP Attribute</td>
</tr>
<tr>
<td></td>
<td>• Optional Attribute Error</td>
</tr>
<tr>
<td></td>
<td>• Invalid Network Field</td>
</tr>
<tr>
<td></td>
<td>• Malformed AS_PATH</td>
</tr>
<tr>
<td></td>
<td>• Hold Timer Expired</td>
</tr>
<tr>
<td></td>
<td>• Finite State Machine Error</td>
</tr>
<tr>
<td></td>
<td>• Rcv Notification</td>
</tr>
<tr>
<td>Last Connection Reset Reason (cont.)</td>
<td>Reasons specific to the Brocade implementation:</td>
</tr>
<tr>
<td></td>
<td>• Reset All Peer Sessions</td>
</tr>
<tr>
<td></td>
<td>• User Reset Peer Session</td>
</tr>
<tr>
<td></td>
<td>• Port State Down</td>
</tr>
<tr>
<td></td>
<td>• Peer Removed</td>
</tr>
<tr>
<td></td>
<td>• Peer Shutdown</td>
</tr>
<tr>
<td></td>
<td>• Peer AS Number Change</td>
</tr>
<tr>
<td></td>
<td>• Peer AS Confederation Change</td>
</tr>
<tr>
<td></td>
<td>• TCP Connection KeepAlive Timeout</td>
</tr>
<tr>
<td></td>
<td>• TCP Connection Closed by Remote</td>
</tr>
<tr>
<td></td>
<td>• TCP Data Stream Error Detected</td>
</tr>
<tr>
<td>Notification Sent</td>
<td>If the device receives a NOTIFICATION message from the neighbor, the message contains an error code corresponding to one of the following errors. Some errors have subcodes that clarify the reason for the error. Where applicable, the subcode messages are listed underneath the error code messages.</td>
</tr>
<tr>
<td></td>
<td>• Message Header Error:</td>
</tr>
<tr>
<td></td>
<td>- Connection Not Synchronized</td>
</tr>
<tr>
<td></td>
<td>- Bad Message Length</td>
</tr>
<tr>
<td></td>
<td>- Bad Message Type</td>
</tr>
<tr>
<td></td>
<td>- Unspecified</td>
</tr>
<tr>
<td></td>
<td>• Open Message Error:</td>
</tr>
<tr>
<td></td>
<td>- Unsupported Version</td>
</tr>
<tr>
<td></td>
<td>- Bad Peer As</td>
</tr>
<tr>
<td></td>
<td>- Bad BGP4 Identifier</td>
</tr>
<tr>
<td></td>
<td>- Unsupported Optional Parameter</td>
</tr>
<tr>
<td></td>
<td>- Authentication Failure</td>
</tr>
<tr>
<td></td>
<td>- Unacceptable Hold Time</td>
</tr>
<tr>
<td></td>
<td>- Unspecified</td>
</tr>
<tr>
<td></td>
<td>• Update Message Error:</td>
</tr>
<tr>
<td></td>
<td>- Malformed Attribute List</td>
</tr>
<tr>
<td></td>
<td>- Unrecognized Attribute</td>
</tr>
<tr>
<td></td>
<td>- Missing Attribute</td>
</tr>
<tr>
<td></td>
<td>- Attribute Flag Error</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|              | - Attribute Length Error  
|              | - Invalid Origin Attribute  
|              | - Invalid NextHop Attribute  
|              | - Optional Attribute Error  
|              | - Invalid Network Field  
|              | - Malformed AS Path  
|              | - Unspecified  
|              |  
|              | • Hold Timer Expired  
|              | • Finite State Machine Error  
|              | • Cease  
|              | • Unspecified  

### Notification Received
Refer to details for the field Notification Sent.

### TCP Connection state
The state of the connection with the neighbor. The connection can have one of the following states:

- **LISTEN** - Waiting for a connection request.
- **SYN-SENT** - Waiting for a matching connection request after having sent a connection request.
- **SYN-RECEIVED** - Waiting for a confirming connection request acknowledgment after having both received and sent a connection request.
- **ESTABLISHED** - Data can be sent and received over the connection. This is the normal operational state of the connection.
- **FIN-WAIT-1** - Waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent.
- **FIN-WAIT-2** - Waiting for a connection termination request from the remote TCP.
- **CLOSE-WAIT** - Waiting for a connection termination request from the local user.
- **CLOSING** - Waiting for a connection termination request acknowledgment from the remote TCP.
- **LAST-ACK** - Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request).
- **TIME-WAIT** - Waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request.
- **CLOSED** - There is no connection state.

### Byte Sent
The number of bytes sent.

### Byte Received
The number of bytes received.

### Local host
The IP address of the device.

### Local port
The TCP port the device is using for the BGP4 TCP session with the neighbor.

### Remote host
The IP address of the neighbor.

### Remote port
The TCP port the neighbor is using for the BGP4 TCP session with the device.
<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISentSeq</td>
<td>The initial send sequence number for the session.</td>
</tr>
<tr>
<td>SendNext</td>
<td>The next sequence number to be sent.</td>
</tr>
<tr>
<td>TotUnAck</td>
<td>The number of sequence numbers sent by the device that have not been acknowledged by the neighbor.</td>
</tr>
<tr>
<td>TotSent</td>
<td>The number of sequence numbers sent to the neighbor.</td>
</tr>
<tr>
<td>Retrans</td>
<td>The number of sequence numbers that the device retransmitted because they were not acknowledged.</td>
</tr>
<tr>
<td>UnAckSeq</td>
<td>The current acknowledged sequence number.</td>
</tr>
<tr>
<td>IRcvSeq</td>
<td>The initial receive sequence number for the session.</td>
</tr>
<tr>
<td>RcvNext</td>
<td>The next sequence number expected from the neighbor.</td>
</tr>
<tr>
<td>SendWnd</td>
<td>The size of the send window.</td>
</tr>
<tr>
<td>TotalRcv</td>
<td>The number of sequence numbers received from the neighbor.</td>
</tr>
<tr>
<td>DupliRcv</td>
<td>The number of duplicate sequence numbers received from the neighbor.</td>
</tr>
<tr>
<td>RcvWnd</td>
<td>The size of the receive window.</td>
</tr>
<tr>
<td>SendQue</td>
<td>The number of sequence numbers in the send queue.</td>
</tr>
<tr>
<td>RcvQue</td>
<td>The number of sequence numbers in the receive queue.</td>
</tr>
<tr>
<td>CngstWnd</td>
<td>The number of times the window has changed.</td>
</tr>
</tbody>
</table>

### Examples

This example shows sample output from the show ip bgp neighbors command.

```bash
device# show ip bgp neighbors

's': Data in InQueue '->': Data in OutQueue ' ': Clearing
'*': Update Policy 'c': Group change 'p': Group change Pending
'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1   IP Address: 60.60.60.20, AS: 200 (IBGP), RouterID: 60.60.60.20, VRF: default-vrf
State: ESTABLISHED, Time: 4h3m28s, KeepAliveTime: 60, HoldTime: 180
    KeepAliveTimer Expire in 0 seconds, HoldTimer Expire in 159 seconds
Minimal Route Advertisement Interval: 0 seconds
    RefreshCapability: Received
Address Family : IPV4 Unicast
    Configured with Add-Path(send receive)capability
    Received Add-Path (send receive)capability in open msg
    Negotiated Add-Path(send receive)capability
Messages:    Open        Update      KeepAlive   Notification   Refresh-Req
            Sent    : 1           1           275         0              0
            Received: 1           1           275         0              0
Last Update Time: NLRI Withdraw NLRI Withdraw
    Tx: 4h3m28s --- Rx: 4h3m28s ---
```
This example shows sample output from the show ip bgp neighbors command when an IP address is specified.

```
device> show ip bgp neighbors 10.4.0.2
Total number of BGP neighbors:
 1  IP Address: 10.4.0.2, AS: 5 (EBGP), RouterID: 10.0.0.1
  Description: neighbor 10.4.0.2
Local AS: 101
State: ESTABLISHED, Time: 0h1m0s, KeepAliveTime: 0, HoldTime: 0
  PeerGroup: pg1
  Multihop-EBGP: yes, ttl: 1
  RouteReflectorClient: yes
  SendCommunity: yes
  NextHopSelf: yes
  DefaultOrigin: yes (default sent)
  MaximumPrefixLimit: 90000
  RemovePrivateAs: : yes
  RefreshCapability: Received
Route Filter Policies:
  Distribute-list: (out) 20
  Filter-list: (in) 30
  Prefix-list: (in) pf1
  Route-map: (in) setnp1 (out) setnp2
Messages:    Open    Update  KeepAlive Notification Refresh-Req
  Sent    : 1       1       1         0            0
  Received: 1       8       1         0            0
Last Update Time: NLRI       Withdraw          NLRI       Withdraw
  Tx: 0h0m59s    ---           Rx: 0h0m59s    ---
Last Connection Reset Reason:Unknown
Notification Sent: Unspecified
Notification Received: Unspecified
TCP Connection state: ESTABLISHED
  Local host:  10.4.0.1, Local  Port: 179
  Remote host: 10.4.0.2, Remote Port: 8053
  ISentSeq:  52837276  SendNext:  52837392  TotUnAck:          0
  TotSent:  116  ReTrans:           0  UnAckSeq:   52837392
  IRcvSeq:  2155052043  RcvNext:  2155052536  SendWnd:       16384
  TotalRcv:        493  DupliRcv:          0  RcvWnd:        16384
  SendQue:           0  RcvQue:            0  CngstWnd:       1460
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>The command was modified. Description codes were added to display output.</td>
</tr>
<tr>
<td>6.0.0</td>
<td>This command was modified to include BGP add path configuration status.</td>
</tr>
</tbody>
</table>
show ip bgp neighbors advertised-routes
Displays the routes that the device has advertised to the neighbor during the current BGP4 session.

Syntax
show ip bgp neighbors ip-addr advertised-routes [ detail | / mask-bits ]

Parameters
ip-addr
IPv4 address of a neighbor in dotted-decimal notation.
detail
Specifies detailed information.
mask-bits
Number of mask bits in CIDR notation.

Modes
User EXEC mode

Examples
This example displays the routes the device has advertised to a specified neighbor.

device# show ip bgp neighbors 192.168.4.211 advertised-routes

There are 2 routes advertised to neighbor 192.168.4.211

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST I:IBGP L:LOCAL

Network Next Hop Metric LocPrf Weight Status
1 10.102.0.0/24 192.168.2.102 12 32768 BL
2 10.200.1.0/24 192.168.2.102 0 32768 BL
show ip bgp neighbors flap-statistics

Displays the route flap statistics for routes received from or sent to a BGP4 neighbor.

Syntax

show ip bgp neighbors ip-addr flap-statistics

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

Modes

User EXEC mode
show ip bgp neighbors last-packet-with-error

Displays the last packets with an error from BGP4 neighbors of the device.

Syntax

```
show ip bgp neighbors ip-addr last-packet-with-error [ decode ]
```

Parameters

- **ip-addr**
  IPv4 address of a neighbor in dotted-decimal notation.

- **decode**
  Decodes the last packet that contained an error from any of a device’s neighbors.

Modes

User EXEC mode
**show ip bgp neighbors received**
Displays Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

**Syntax**
```
show ip bgp neighbors ip-addr received { extended-community | prefix-filter }
```

**Parameters**
- **ip-addr**
  IPv4 address of a neighbor in dotted-decimal notation.
- **extended-community**
  Displays the results for ORFs that use the BGP Extended Community Attribute.
- **prefix-filter**
  Displays the results for ORFs that are prefix-based.

**Modes**
User EXEC mode

**Examples**
This example displays sample output for the `show ip bgp neighbors received` command when the `prefix-filter` keyword is used.

```
device# show ip bgp neighbor 10.10.10.1 received prefix-filter
ip prefix-list 10.10.10.1: 4 entries
  seq 5 permit 10.10.0.0/16 ge 18 le 28
  seq 10 permit 10.20.10.0/24
  seq 15 permit 10.0.0.0/8 le 32
  seq 20 permit 10.10.0.0/16 ge 18
```
show ip bgp neighbors received-routes

Lists all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

Syntax

```
show ip bgp neighbors ip-addr received-routes [ detail ] [ vrf vrf-name ]
```

Parameters

- `ip-addr`
  IPv4 address of a neighbor in dotted-decimal notation.

- `detail`
  Displays detailed route information.

Modes

User EXEC mode

Examples

This example displays the details of route updates for VRF instance 'red'.

```
device# show ip bgp neighbor 10.168.4.106 received-routes
  There are 9745 received routes from neighbor 10.168.4.106
  Searching for matching routes, use ^C to quit...
Prefix Next Hop     MED   LocPrf Weight Status
1  10.3.0.0/8  10.168.4.106 100    0      BE
    AS_PATH: 65001 4355 701 8
2  10.4.0.0/8  10.168.4.106 100    0      BE
    AS_PATH: 65001 4355 1
3  10.6.0.0/22 10.168.4.106 100    0      BE
    AS_PATH: 65001 4355 7 189
4  10.6.0.0/22 10.168.4.106 100    0      BE
```
show ip bgp neighbors rib-out-routes

Displays information about display the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

Syntax

show ip bgp neighbors ip-addr rib-out-routes [ detail ] [ip-addr [ / mask ] ]

Parameters

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

last-packet-with-error
Displays the last packet with an error.

routes-summary
Displays routes received, routes accepted, number of routes advertised by peer, and so on.

Modes
User EXEC mode

Examples

This example shows information about the routes that the device either has most recently sent, or is about to send, to a specified neighbor and a specified destination network

device> show ip bgp neighbor 192.168.4.211 rib-out-routes 192.168.1.0/24

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST I:IBGP L:LOCAL
Prefix           Next Hop       Metric     LocPrf     Weight Status
1      10.200.1.0/24       0.0.0.0         0          101        32768  BL
show ip bgp routes community
  Displays BGP4 route information that is filtered by community and other options.

Syntax
  show ip bgp routes community { num | aa:nn | internet | local-as | no-advertise | no-export }

Parameters
  community
    Displays routes filtered by a variety of communities.
  num
    Specifies a community number n in the range from 1 to 4294967200.
  aa:nn
    Specifies an autonomous system-community number.
  internet
    Displays routes for the Internet community.
  local-as
    Displays routes for a local sub-AS within the confederation.
  no-advertise
    Displays routes with this community that cannot be advertised to any other BGP4 devices at all.
  no-export
    Displays routes for the community of sub-ASs within a confederation.

Modes
  User EXEC mode
show ip bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4 neighbors.

Syntax

```
show ip bgp neighbors ip-addr routes
show ip bgp neighbors ip-addr routes { best | not-installed-best | unreachable }
show ip bgp neighbors ip-addr routes detail { best | not-installed-best | unreachable }
```

Parameters

- `ip-addr` IPv4 address of a neighbor in dotted-decimal notation.
- `best` Displays routes received from the neighbor that are the best BGP4 routes to their destination.
- `not-installed-best` Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in the route table because the device received better routes from other sources.
- `unreachable` Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

Modes

User EXEC mode

Examples

The following example shows sample output for the `show ip bgp neighbors routes` command.

```
device# show ip bgp neighbors 192.168.4.106 routes

There are 97345 received routes from neighbor 192.168.4.106
Searching for matching routes, use ^C to quit...

status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED

status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED

Prefix       Next Hop              MED     LocPrf   Weight  Status
------------- -------------          ------  -------   -------  ------
1  10.3.0.0/8     192.168.4.106   100     0       BE
   AS_PATH: 65001 4355 701 8
2  10.4.0.0/8     192.168.4.106   100     0       BE
   AS_PATH: 65001 4355 1
3  10.60.212.0/22  192.168.4.106   100     0       BE
   AS_PATH: 65001 4355 701 1 189
4  10.6.0.0/8     192.168.4.106   100     0       BE
   AS_PATH: 65001 4355 701 1 189
...```

Show Commands

NetIron Command Line Interface (CLI) Reference Guide
S3-1004199-02
show ip bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4 neighbors.

Syntax

```
show ip bgp neighbors ip-addr routes-summary
```

Parameters

- `ip-addr`
  
  IPv4 address of a neighbor in dotted-decimal notation.

Modes

User EXEC mode

Command Output

The `show ip bgp neighbors routes-summary` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the neighbor.</td>
</tr>
<tr>
<td>Routes Received</td>
<td>How many routes the device has received from the neighbor during the current BGP4 session:</td>
</tr>
<tr>
<td></td>
<td>▪ Accepted or Installed - Number of received routes the device accepted and installed in the BGP4 route table.</td>
</tr>
<tr>
<td></td>
<td>▪ Filtered or Kept - Number of routes that were filtered out, but were retained in memory for use by the soft reconfiguration feature.</td>
</tr>
<tr>
<td></td>
<td>▪ Filtered - Number of received routes filtered out.</td>
</tr>
<tr>
<td>Routes Selected as BEST Routes</td>
<td>The number of routes that the device selected as the best routes to their destinations.</td>
</tr>
<tr>
<td>BEST Routes not Installed in IP Forwarding Table</td>
<td>The number of routes received from the neighbor that are the best BGP4 routes to their destinations, but were not installed in the IP route table because the device received better routes from other sources (such as OSPF, RIP, or static IP routes).</td>
</tr>
<tr>
<td>Unreachable Routes</td>
<td>The number of routes received from the neighbor that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next-hop.</td>
</tr>
<tr>
<td>History Routes</td>
<td>The number of routes that are down but are being retained for route flap dampening purposes.</td>
</tr>
<tr>
<td>NLRIs Received in Update Message</td>
<td>The number of routes received in Network Layer Reachability (NLSI) format in UPDATE messages:</td>
</tr>
<tr>
<td></td>
<td>▪ Withdraws - Number of withdrawn routes the device has received.</td>
</tr>
<tr>
<td></td>
<td>▪ Replacements - Number of replacement routes the device has received.</td>
</tr>
<tr>
<td>NLRIs Discarded due to</td>
<td>Indicates the number of times the device discarded an NLRI for the neighbor due to the following reasons:</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>· Maximum Prefix Limit - The configured maximum prefix amount had been reached.</td>
<td></td>
</tr>
<tr>
<td>· AS Loop - An AS loop occurred. An AS loop occurs when the BGP4 AS-path attribute contains the local AS number.</td>
<td></td>
</tr>
<tr>
<td>· maxas-limit aspath - The number of route entries discarded because the AS path exceeded the configured maximum length or exceeded the internal memory limits.</td>
<td></td>
</tr>
<tr>
<td>· Invalid Nexthop - The next-hop value was not acceptable.</td>
<td></td>
</tr>
<tr>
<td>· Duplicated Originator_ID - The originator ID was the same as the local device ID.</td>
<td></td>
</tr>
<tr>
<td>· Cluster_ID - The cluster list contained the local cluster ID, or the local device ID if the cluster ID is not configured.</td>
<td></td>
</tr>
</tbody>
</table>

### Routes Advertised

- The number of routes the device has advertised to this neighbor:
  - To be Sent - The number of routes queued to send to this neighbor.
  - To beWithdrawn - The number of NLRIs for withdrawing routes the device has queued to send to this neighbor in UPDATE messages.

### NLRIs Sent in Update Message

- The number of NLRIs for new routes the device has sent to this neighbor in UPDATE messages:
  - Withdraws - Number of routes the device has sent to the neighbor to withdraw.
  - Replacements - Number of routes the device has sent to the neighbor to replace routes the neighbor already has.

### Peer Out of Memory Count for

- Statistics for the times the device has run out of BGP4 memory for the neighbor during the current BGP4 session:
  - Receiving Update Messages - The number of times UPDATE messages were discarded because there was no memory for attribute entries.
  - Accepting Routes (NLRI) - The number of NLRIs discarded because there was no memory for NLRI entries. This count is not included in the Receiving Update Messages count.
  - Attributes - The number of times there was no memory for BGP4 attribute entries.
  - Outbound Routes (RIB-out) - The number of times there was no memory to place a “best” route into the neighbor route information base (Adj-RIB-Out) for routes to be advertised.
Examples

The following example displays route summary information received in UPDATE messages.

device# show ip bgp neighbor 10.168.4.211 routes-summary

1   IP Address: 10.168.4.211
Routes Accepted/Installed:1, Filtered/Kept:11, Filtered:11
   Routes Selected as BEST Routes:1
   BEST Routes not Installed in IP Forwarding Table:0
   Unreachable Routes (no IGP Route for NEXTHOP):0
   History Routes:0

NLRIs Received in Update Message:24, Withdraws:0 (0), Replacements:1
   NLRIs Discarded due to
      Maximum Prefix Limit:0, AS Loop:0
      Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
      Duplicated Originator_ID:0, Cluster_ID:0

Routes Advertised:0, To be Sent:0, To be Withdrawn:0
NLRIs Sent in Update Message:0, Withdraws:0, Replacements:0

Peer Out of Memory Count for:
   Receiving Update Messages:0, Accepting Routes(NLRI):0
   Attributes:0, Outbound Routes(RIB-out):0
show ip bgp peer-group

Displays peer-group information.

Syntax

show ip bgp peer-group peer-group-name

Parameters

peer-group-name

Specifies a peer group name.

Modes

User EXEC mode

Usage Guidelines

Only the parameters that have values different from their defaults are listed.

Examples

This example shows sample output from the show ip bgp peer-group command.

device# show ip bgp peer-group STR
1    BGP peer-group is STR
     Address family : IPV4 Unicast
        activate
     Address family : IPV4 Multicast
        no activate
     Address family : IPV6 Unicast
        no activate
     Address family : IPV6 Multicast
        no activate
     Address family : VPNV4 Unicast
        no activate
     Address family : L2VPN VPLS
        no activate
Members:
   IP Address: 10.1.1.1, AS: 5
show ip bgp routes
Displays statistics for the routes in the BGP4 route table of a device.

Syntax
show ip bgp routes [ detail ] [ num | ip-address/prefix | age num | as-path-access-list name | as-path-filter number | best | cidr-only | community-access-list name | community-filter number | community-reg-expression expression | local | neighbor ip-addr | nexthop ip-addr | no-best | not-installed-best | prefix-list string | regular-expression name | route-map name | summary | unreachable ]

Parameters

detail
Displays detailed information.

num
Table entry at which the display starts. For example, if you want to list entries beginning with table entry 100, specify 100.

ip-address/prefix
Specifies an IP address and prefix.

age num
Displays BGP4 route information that is filtered by age.

as-path-access-list name
Displays BGP4 route information that is filtered by autonomous system (AS)-path access control list (ACL).

as-path-filter number
Displays BGP4 route information that is filtered using the specified AS-path filter.

best
Displays BGP4 route information that the device selected as best routes.

cidr-only
Displays BGP4 routes whose network masks do not match their class network length.

community-access-list name
Displays BGP4 route information for an AS-path community access list.

community-filter number
Displays BGP4 route information that matches a specific community filter.

community-reg-expression expression
Displays BGP4 route information for an ordered community list regular expression.

local
Displays BGP4 route information about selected local routes.

neighbor ip-addr
Displays BGP4 route information about selected BGP neighbors.

nexthop ip-addr
Displays BGP4 route information about routes that are received from the specified next hop.

no-best
Displays BGP4 route information that the device selected as not best routes.

not-installed-best
Displays BGP4 route information about best routes that are not installed.

prefix-list string
Displays BGP4 route information that is filtered by a prefix list.

regular-expression name
Displays BGP4 route information about routes that are associated with the specified regular expression.

route-map name
Displays BGP4 route information about routes that use the specified route map.

summary
Displays BGP4 summary route information.

unreachable
Displays BGP4 route information about routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.

Modes
User EXEC mode

Command Output
The show ip bgp routes command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of BGP4 routes (NLRIs) Installed</td>
<td>Number of BGP4 routes the device has installed in the BGP4 route table.</td>
</tr>
<tr>
<td>Distinct BGP4 destination networks</td>
<td>Number of destination networks the installed routes represent. The BGP4 route table can have multiple routes to the same network.</td>
</tr>
<tr>
<td>Filtered BGP4 routes for soft reconfig</td>
<td>Number of route updates received from soft-reconfigured neighbors or peer groups that have been filtered out but retained.</td>
</tr>
<tr>
<td>Routes originated by this device</td>
<td>Number of routes in the BGP4 route table that this device originated.</td>
</tr>
<tr>
<td>Routes selected as BEST routes</td>
<td>Number of routes in the BGP4 route table that this device has selected as the best routes to the destinations.</td>
</tr>
<tr>
<td>BEST routes not installed in IP forwarding table</td>
<td>Number of BGP4 routes that are the best BGP4 routes to their destinations but were not installed in the IP route table because the device received better routes from other sources (such as OSPF, RIP, or static IP routes).</td>
</tr>
<tr>
<td>Unreachable routes (no IGP route for NEXTHOP)</td>
<td>Number of routes in the BGP4 route table whose destinations are unreachable because the next-hop is unreachable.</td>
</tr>
<tr>
<td>IBGP routes selected as best routes</td>
<td>Number of &quot;best&quot; routes in the BGP4 route table that are IBGP routes.</td>
</tr>
<tr>
<td>EBGP routes selected as best routes</td>
<td>Number of &quot;best&quot; routes in the BGP4 route table that are EBGP routes.</td>
</tr>
</tbody>
</table>
Examples

The following example shows sample output from the `show ip bgp routes` command.

```
device# show ip bgp routes

Total number of BGP Routes: 2000

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>MED</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 150.150.150.0/24</td>
<td>103.103.1.1</td>
<td>2</td>
<td>100</td>
<td>0</td>
<td>BEx</td>
</tr>
<tr>
<td>2 150.150.150.0/24</td>
<td>103.103.2.1</td>
<td>3</td>
<td>100</td>
<td>0</td>
<td>E</td>
</tr>
<tr>
<td>3 150.150.150.0/24</td>
<td>103.103.3.1</td>
<td>4</td>
<td>100</td>
<td>0</td>
<td>E</td>
</tr>
<tr>
<td>4 150.150.150.0/24</td>
<td>103.103.4.1</td>
<td>5</td>
<td>100</td>
<td>0</td>
<td>E</td>
</tr>
<tr>
<td>5 150.150.150.0/24</td>
<td>103.103.5.1</td>
<td>6</td>
<td>100</td>
<td>0</td>
<td>E</td>
</tr>
</tbody>
</table>
```

The following example shows sample output from the `show ip bgp routes` command when the `detail` keyword is used.

```
device# show ip bgp routes detail

Total number of BGP Routes: 2

1  Prefix: 10.5.0.0/24,  Status: BME,  Age: 0h28m28s
    NEXT_HOP: 10.1.1.2,  Learned from Peer: 10.1.0.2 (5)
    LOCAL_PREF: 101,  MED: 0,  ORIGIN: igp,  Weight: 10
    AS_PATH: 5
    Adj_RIB_out count: 4,  Admin distance 20
```

The following example shows sample output from the `show ip bgp routes` command when the `summary` keyword is used.

```
device> show ip bgp routes summary

Total number of BGP routes (NLRIs) Installed : 20
Distinct BGP destination networks            : 20
Filtered BGP routes for soft reconfig        : 100178
Routes originated by this router             : 2
Routes selected as best routes               : 19
BEST routes not installed in IP forwarding table : 1
Unreachable routes (no IGP route for NEXTHOP) : 1
IBGP routes selected as best routes          : 0
EBGP routes selected as best routes          : 17
```

The following example shows sample output from the `show ip bgp routes` command when the `unreachable` keyword is used.

```
device> show ip bgp routes unreachable

Searching for matching routes, use ^C to quit...


<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 10.8.0.0/24</td>
<td>192.168.5.1</td>
<td>0</td>
<td>101</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
    AS_PATH: 65001 4355 1
```
The following example shows sample output from the `show ip bgp routes` command when an IP address is specified.

```
device> show ip bgp route 10.3.4.0

Number of BGP Routes matching display condition : 1
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network       Next Hop      Metric LocPrf Weight Path  
*>  10.3.4.0/24   192.168.4.106        100    0      65001 4355 1 1221 ?

Last update to IP routing table: 0h11m38s, 1 path(s) installed:
  Gateway           Port
  192.168.2.1       2/1

Route is advertised to 1 peers:
  10.20.20.2(65300)
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>Command output was modified to include details about BGP additional paths.</td>
</tr>
</tbody>
</table>
show ip bgp summary
Displays summarized information about the status of all BGP connections.

Syntax
show ip bgp summary

Modes
User EXEC mode

Usage Guidelines
If a BGP4 peer is not configured for an address-family, the peer information is not displayed. If a BGP4 peer is configured for an address-family but not negotiated for an address-family after the BGP4 peer is in the established state, the show ip bgp summary command output shows (NoNeg) at the end of the line for this peer.

Command Output
The show ip bgp summary command displays the following information:

<table>
<thead>
<tr>
<th>This field</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The device ID.</td>
</tr>
<tr>
<td>Local AS Number</td>
<td>The BGP4 AS number for the device.</td>
</tr>
<tr>
<td>Confederation Identifier</td>
<td>The AS number of the confederation in which the device resides.</td>
</tr>
<tr>
<td>Confederation Peers</td>
<td>The numbers of the local autonomous systems contained in the confederation. This list matches the confederation peer list you configure on the device.</td>
</tr>
<tr>
<td>Maximum Number of Paths Supported for Load Sharing</td>
<td>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.</td>
</tr>
<tr>
<td>Number of Neighbors Configured</td>
<td>The number of BGP4 neighbors configured on this device, and currently in established state.</td>
</tr>
<tr>
<td>Number of Routes Installed</td>
<td>The number of BGP4 routes in the device BGP4 route table and the route or path memory usage.</td>
</tr>
<tr>
<td>Number of Routes Advertising to All Neighbors</td>
<td>The total of the RtSent and RTosend columns for all neighbors, the total number of unique ribout group entries, and the amount of memory used by these groups.</td>
</tr>
<tr>
<td>Number of Attribute Entries Installed</td>
<td>The number of BGP4 route-attribute entries in the device route-attribute table and the amount of memory used by these entries.</td>
</tr>
<tr>
<td>Neighbor Address</td>
<td>The IP addresses of the BGP4 neighbors for this device.</td>
</tr>
<tr>
<td>AS#</td>
<td>The AS number.</td>
</tr>
<tr>
<td>State</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td>This field</td>
<td>Displays</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>session has gone down and the software is clearing or removing routes.</td>
</tr>
<tr>
<td>ADMND</td>
<td>The neighbor has been administratively shut down.</td>
</tr>
<tr>
<td>CONNECT</td>
<td>BGP4 is waiting for the connection process for the TCP neighbor session to be completed.</td>
</tr>
<tr>
<td>ACTIVE</td>
<td>BGP4 is waiting for a TCP connection from the neighbor.</td>
</tr>
<tr>
<td>Note</td>
<td>If the state frequently changes between CONNECT and ACTIVE, there may be a problem with the TCP connection.</td>
</tr>
<tr>
<td>OPEN SENT</td>
<td>BGP4 is waiting for an Open message from the neighbor.</td>
</tr>
<tr>
<td>OPEN CONFIRM</td>
<td>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.</td>
</tr>
<tr>
<td>ESTABLISHED</td>
<td>BGP4 is ready to exchange UPDATE packets with the neighbor.</td>
</tr>
</tbody>
</table>

**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. |

<table>
<thead>
<tr>
<th>Time</th>
<th>The time that has passed since the state last changed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepted</td>
<td>The number of routes received from the neighbor that this device installed in the BGP4 route table. Usually, this number is lower than</td>
</tr>
</tbody>
</table>
This field Displays
the RoutesRcvd number. The difference indicates that this device filtered out some of the routes received in the UPDATE messages.

Filtered
The routes or prefixes that have been filtered out:
- If soft reconfiguration is enabled, this field shows how many routes were filtered out (not placed in the BGP4 route table) but retained in memory.
- If soft reconfiguration is not enabled, this field shows the number of BGP4 routes that have been filtered out.

Sent
The number of BGP4 routes the device has sent to the neighbor.

ToSend
The number of routes the device has queued to advertise and withdraw to a neighbor.

Examples
This example displays sample output from the `show ip bgp summary` command.

device> show ip bgp summary
BGP4 Summary
Router ID: 7.7.7.7 Local AS Number: 100
Confederation Identifier: not configured
Confederation Peers:
Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
Number of Neighbors Configured: 1, UP: 1
Number of Routes Installed: 0
Number of Routes Advertising to All Neighbors: 0 (0 entries)
Number of Attribute Entries Installed: 0
'+': Data in InQueue '>': Data in OutQueue '-': Clearing
'^': Update Policy 'c': Group change 'p': Group change Pending
'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting
Neighbor Address AS# State Time Rt:Accepted Filtered Sent ToSend
10.1.1.8 100 ESTAB 0h 9m16s 0 0 0 0

History
Release version Command history
5.9.00 The command was modified. Description codes were added to display output.
show ip bgp vrf neighbors
Displays configuration information and statistics for BGP4 neighbors of the device for a virtual routing and forwarding (VRF) instance.

Syntax

```
show ip bgp vrf vrf-name neighbors [ ip-addr ]
show ip bgp vrf vrf-name neighbors last-packet-with-error
show ip bgp vrf vrf-name neighbors routes-summary
show ip bgp vrf vrf-name neighbors ip-addr advertised-routes [ detail ] [ ip address /mask ]
show ip bgp vrf vrf-name neighbors ip-addr flap-statistics
show ip bgp vrf vrf-name neighbors ip-addr last-packet-with-error [ decode ]
show ip bgp vrf vrf-name neighbors ip-addr received [ prefix-filter ]
show ip bgp vrf vrf-name neighbors ip-addr received-routes [ detail ]
show ip bgp vrf vrf-name neighbors ip-addr rib-out-routes [ detail ] [ ipv6 address /mask ]
show ip bgp vrf vrf-name neighbors ip-addr routes
show ip bgp vrf vrf-name neighbors ip-addr routes { best | not-installed-best | unreachable }
show ip bgp vrf vrf-name neighbors ip-addr routes detail { best | not-installed-best | unreachable }
show ip bgp vrf vrf-name neighbors ip-addr routes-summary
```

Parameters

- **vrf-name**
  Specifies the name of a VRF instance.

- **neighbors**
  Specifies a neighbor.

- **ip-addr**
  IPv4 address of a neighbor in dotted-decimal notation.

- **last-packet-with-error**
  Displays the last packet with an error.

- **routes-summary**
  Displays routes received, routes accepted, number of routes advertised by peer, and so on.

- **advertised-routes**
  Specifies the routes that the device has advertised to the neighbor during the current BGP4 session.

- **detail**
  Specifies detailed information.

- **ip address /mask**
  Specifies an IP address and mask.
**flap-statistics**
Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

**last-packet-with-error**
Specifies the last packet with an error.

**decode**
Decodes the last packet that contained an error from any of a device’s neighbors.

**received**
Specifies Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

**prefix-filter**
Displays the results for ORFs that are prefix-based.

**received-routes**
Specifies all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

**rib-out-routes**
Displays information about the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and specific destination networks.

**routes**
Displays a variety of route information received in UPDATE messages from BGP4 neighbors.

**best**
Displays routes received from the neighbor that are the best BGP4 routes to their destination.

**not-installed-best**
Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in the route table because the device received better routes from other sources.

**unreachable**
Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

**routes-summary**
Displays all route information received in UPDATE messages from BGP4 neighbors.

**Modes**
User EXEC mode
show ip bgp vrf routes

Displays statistics for the routes in the BGP4 route table of a device for a virtual routing and forwarding (VRF) instance.

Syntax

```
show ip bgp vrf vrf-name routes [ detail ] [ num | ip-address/prefix | age num | as-path-access-list name | as-path-filter number | best | cidr-only | community-access-list name | community-filter number | community-reg-expression expression | local | neighbor ip-addr | nexthop ip-addr | no-best | not-installed-best | prefix-list string | regular-expression name | route-map name | summary | unreachable ]
```

Parameters

- **vrf-name**
  Specifies the name of a VRF instance.
- **detail**
  Displays detailed information.
- **num**
  Table entry at which the display starts. For example, if you want to list entries beginning with table entry 100, specify 100.
- **ip-address/prefix**
  Specifies an IP address and prefix.
- **age num**
  Displays BGP4 route information that is filtered by age.
- **as-path-access-list name**
  Displays BGP4 route information that is filtered by autonomous system (AS)-path access control list (ACL).
- **as-path-filter number**
  Displays BGP4 route information that is filtered using the specified AS-path filter.
- **best**
  Displays BGP4 route information that the device selected as best routes.
- **cidr-only**
  Displays BGP4 routes whose network masks do not match their class network length.
- **community-access-list name**
  Displays BGP4 route information for an AS-path community access list.
- **community-filter number**
  Displays BGP4 route information that matches a specific community filter.
- **community-reg-expression expression**
  Displays BGP4 route information for an ordered community list regular expression.
- **local**
  Displays BGP4 route information about selected local routes.
- **neighbor ip-addr**
  Show Commands
Displays BGP4 route information about selected BGP neighbors.

**nexthop** ip-addr
Displays BGP4 route information about routes that are received from the specified next hop.

**no-best**
Displays BGP4 route information that the device selected as not best routes.

**not-installed-best**
Displays BGP4 route information about best routes that are not installed.

**prefix-list** string
Displays BGP4 route information that is filtered by a prefix list.

**regular-expression** name
Displays BGP4 route information about routes that are associated with the specified regular expression.

**route-map** name
Displays BGP4 route information about routes that use the specified route map.

**summary**
Displays BGP4 summary route information.

**unreachable**
Displays BGP4 route information about routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.

**Modes**
User EXEC mode
show ip bgp vrf

Displays entries in the IPv4 Border Gateway Protocol (BGP4) routing table for a virtual routing and forwarding (VRF) instance.

Syntax

show ip bgp vrf vrf-name
show ip bgp vrf vrf-name ipv6 address /mask [longer-prefixes]
show ip bgp vrf vrf-name ip address /mask [longer-prefixes]
show ip bgp vrf vrf-name attribute-entries
show ip bgp vrf vrf-name dampened-paths
show ip bgp vrf vrf-name filtered-routes [detail] [ip-addr / mask] [longer-prefixes] | as-path-access-list name | prefix-list name
show ip bgp vrf vrf-name flap-statistics
show ip bgp vrf vrf-name flap-statistics ip-addr /mask [longer-prefix]
show ip bgp vrf vrf-name flap-statistics as-path-filter name
show ip bgp vrf vrf-name flap-statistics neighbor ip-addr
show ip bgp vrf vrf-name flap-statistics regular-expression name
show ip bgp vrf vrf-name nexthop [ip-addr | reachable | unreachable]
show ip bgp vrf vrf-name peer-group peer-group-name
show ip bgp vrf vrf-name summary

Parameters

vrf-name
  Specifies the name of a VRF instance.
ipv6 address /mask
  Specifies an IPv6 address and mask.
longer-prefixes
  Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.
ip address /mask
  Specifies an IP address and mask.
attribute-entries
  Specifies BGP4 route-attribute entries that are stored in device memory.
dampened-paths
  Specifies multiprotocol BGP (MBGP) paths that have been dampened by route-flap dampening.
filtered-routes
  Specifies BGP4 filtered routes that are received from a neighbor or peer group.
detail
Optionally displays detailed route information.

**as-path-access-list** name
Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

**prefix-list** name
Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

**flap-statistics**
Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

**as-path-filter** name
Specifies an AS-path filter.

**neighbor**
Displays flap statistics only for routes learned from the specified neighbor.

```
ip-addr
```
IPv4 address of the neighbor.

**regular-expression**
Specifies a regular expression in the display output on which to filter.

```
name
```
Name of an AS-path filter or regular expression.

**nexthop**
Specifies the configured next hop.

**reachable**
Specifies reachable next hops.

**unreachable**
Specifies unreachable next hops.

**peer-group** peer-group-name
Specifies a peer group.

**summary**
Displays summarized information.

**Modes**
User EXEC mode
show ip http client

Displays information about the http(s) link and request between the http(s)erver and the Brocade device (client).

Syntax

show ip http client

Modes

User EXEC mode.

Usage Guidelines

Command Output

The show ip http client command displays the following information:

<table>
<thead>
<tr>
<th>TABLE 7 Callers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>Session</td>
<td>The session ID</td>
</tr>
<tr>
<td>Username</td>
<td>The username (Blank if none used)</td>
</tr>
<tr>
<td>Server</td>
<td>The server connection number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE 8 Servers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>Connection</td>
<td>The server connection number</td>
</tr>
<tr>
<td>Version</td>
<td>HTTP 1.0 or 1.1</td>
</tr>
<tr>
<td>Transport</td>
<td>TCP or TLS</td>
</tr>
<tr>
<td>Request</td>
<td>Current request number being processed</td>
</tr>
<tr>
<td>IP Address[:Port]</td>
<td>Remote server IPv4 or IPv6 address, and port (if non-default port)</td>
</tr>
</tbody>
</table>

Number | The Request number
Method | GET, PUT, ...
Examples

The following example shows the output from a show ip http client command:

device# show ip http client
Callers:
Session Username Server
1 lab 1

Servers:
Connection Version Transport Request IP Address
1 1.0 TCP 1 10.25.104.10

Requests:
Number Method
1 GET

NOTE
There is no history of prior connections being maintained. Once the file transfer is completed, the HTTP(S) session will be closed, and it will no longer be visible under the Server connections.

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ip interface
Displays useful information about the configuration and status of the IP protocol and its services, on all interfaces.

Syntax
```
show ip interface counters [ [ ethernet slot/port | loopback num ] | [ pos slot/port | tunnel num ] ]
show ip interface ve num [ statistics [ detail | ethernet slot/port | vpls vlan vlan_id ] ]
```

Parameters
- **counters**: Displays the interface level IP counters.
- **ethernet slot/port**: Displays the specified Ethernet interface port.
- **loopback num**: Displays the loopback interface number.
- **pos slot/port**: Displays the POS interface number.
- **tunnel num**: Displays the tunnel interface number.
- **ve num**: Displays the Virtual Ethernet interface number.
- **statistics**: Displays the interface level IP counters.
- **detail**: Displays the interface IP extended counters in detail.
- **ethernet slot/port**: Displays the interface IP counters for the specified port.
- **vpls**: Displays the VPLS-VE end point IP counters.
- **vlan vlan_id**: Displays the specified VPLS-VE end point IP counters.

Modes
EXEC mode

Command Output
The `show ip interface` command displays the following information:
### Output field Description

- **Interface**: The type and the slot and port number of the interface.
- **IP-Address**: The IP address of the interface.
- **OK?**: Whether the IP address is configured on the interface.
- **Method**: Whether the IP address is saved in NVRAM. If you have set the IP address for the interface in the CLI, the Method field is “manual”.
- **Status**: The link status of the interface. If the user has disabled the interface with the `disable` command, the entry in the 'Status' field is “administratively DOWN”. Otherwise, the entry in the 'Status' field is either UP or DOWN.
- **Protocol**: Whether the interface can provide two-way communication. If the IP address is configured and the link status of the interface is up, the entry in the 'Protocol' field is UP. Otherwise, the entry in the 'Protocol' field is DOWN.
- **VRF**: Whether the VRF is configured or set to default.
- **Flag**: Interface flag:
  - U- Unnumbered
  - S- Secondary
  - US- Unnumbered Secondary
  - V- V-VE over VPLS
  - VS- S-VE over VPLS Secondary

### Examples

The following example displays the `show ip interface` command modified to display a flag “V” when the interface is a VE over VPLS interface. This enhancement is on the MP as well as the LP.

```
device# show ip int

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
<th>VRF</th>
<th>FLAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt 1</td>
<td>10.25.106.36</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
<td>default-vrf</td>
<td></td>
</tr>
<tr>
<td>ve 40</td>
<td>10.40.40.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>down</td>
<td>down</td>
<td>default-vrf</td>
<td></td>
</tr>
<tr>
<td>ve 150</td>
<td>10.15.15.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
<td>default-vrf</td>
<td>V</td>
</tr>
<tr>
<td>ve 150</td>
<td>10.20.20.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
<td>default-vrf</td>
<td>V</td>
</tr>
<tr>
<td>ve 150</td>
<td>10.15.15.2</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
<td>default-vrf</td>
<td>VS</td>
</tr>
<tr>
<td>loopback 1</td>
<td>10.1.1.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
<td>default-vrf</td>
<td></td>
</tr>
</tbody>
</table>
```
The following example displays the show ip interface ve num command modified to display ve-type information.

device# show ip interface ve 77
Interface Ve 77
  type: vpls
  vpls-id: 3 (name: a)
  members: vlan 20 – ethe 2/2, vlan 20 – ethe 2/3, vlan 101 – ethe 4/1, peer – 12.12.2.5
  active: vlan 20 – ethe 2/2, vlan 20 – ethe 2/3, peer – 12.12.2.5
  port disabled
  port state: DOWN
  ip address: 77.77.77.77/24
  Port belongs to VRF: default-vrf
  encapsulation: ETHERNET, mtu: 1500
  directed-broadcast-forwarding: disabled
  ip icmp redirect: enabled
  ip local proxy arp: disabled
  ip ignore gratuitous arp: disabled
  No inbound ip access-list is set
  No outbound ip access-list is set
  No Helper Addresses are configured.

The following example displays the show ip interface tunnel num command modified to display the traffic counters for the IPSec IPv4 tunnel.

device# show ip interface tunnel 10
Interface Tunnel 10
  port enabled
  port state: UP
  ip address: 11.11.11.5/24
  Port belongs to VRF: default-vrf
  encapsulation: ETHERNET, mtu: 1431
  directed-broadcast-forwarding: disabled
  ip icmp redirect: enabled
  ip local proxy arp: disabled
  ip ignore gratuitous arp: disabled
  No inbound ip access-list is set
  No outbound ip access-list is set
  No Helper Addresses are configured.
  RxPkts:  100  TxPkts:11200
  RxBytes:150  TxBytes:12544

The following example displays the show ip interface command with the ve num statistics option. This command is only applicable for G2/G3a modules.

device# show ip interface ve 1001 statistics
Extended Routed Counters (only applicable for G2/G3a modules):

<table>
<thead>
<tr>
<th></th>
<th>VPLS Name: instance1001, VPLS Id: 1001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total RxPkts</td>
<td>17</td>
</tr>
<tr>
<td>Total TxPkts</td>
<td>0</td>
</tr>
<tr>
<td>Total RxBytes</td>
<td>3478</td>
</tr>
<tr>
<td>Total TxBytes</td>
<td>0</td>
</tr>
</tbody>
</table>

device# show ip interface ve 1001 statistics detail
VPLS Extended Counters (only applicable for G2/G3a modules):

<table>
<thead>
<tr>
<th></th>
<th>VPLS Name: instance1001, VPLS Id: 1001</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPLS Vlan: vlan 1001</td>
<td></td>
</tr>
<tr>
<td>Interface RxPkts</td>
<td>265</td>
</tr>
<tr>
<td>Interface TxPkts</td>
<td>2170</td>
</tr>
<tr>
<td>Interface RxBytes</td>
<td>37882</td>
</tr>
<tr>
<td>Interface TxBytes</td>
<td>235824</td>
</tr>
</tbody>
</table>
The following example displays the `show ip interface` command with the `ve num statistics detail` option. This command is only applicable for G2/G3a modules.

```
device# show ip interface ve 1001 statistics detail
VPLS Extended Counters (only applicable for G2/G3a modules):
VPLS Name: instance1001, VPLS  Id: 1001
eth 6/6  265              2170             37882            235824
```

The following example displays the `show ip interface` command with the `ve num statistics vpls vlan vlan_id` option. This command is only applicable for G2/G3a modules.

```
device# show ip interface ve 1001 statistics vpls vlan 1001 ethernet 6/6
Extended Routed Counters (only applicable for G2/G3a modules):
VPLS Name: instance1001, VPLS  Id: 1001
Total     RxPkts           TxPkts           RxBytes          TxBytes
           17               0                3478             0
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>The <code>show ip interface</code> command was modified to display a flag &quot;V&quot; if the interface is a VE over VPLS interface. The <code>show ip interface ve</code> command was modified to display VPLS-VE specific information. A new 'Type' field is introduced that shows what type of ve interface it is (VLAN or VPLS). This enhancement is only available for the MP.</td>
</tr>
</tbody>
</table>
show ip mbgp ipv6
Displays IPv6 multicast information.

Syntax

show ip mbgp ipv6 neighbors
show ip mbgp ipv6 neighbors ip-addr advertised-routes [ detail ] [ ipv6 address /mask ]
show ip mbgp ipv6 neighbors ip-addr flap-statistics
show ip mbgp ipv6 neighbors ip-addr last-packet-with-error [ decode ]
show ip mbgp ipv6 neighbors ip-addr received [ prefix-filter ]
show ip mbgp ipv6 neighbors ip-addr received-routes [ detail ]
show ip mbgp ipv6 neighbors ip-addr rib-out-routes [ detail ] [ ipv6 address /mask ]
show ip mbgp ipv6 neighbors ip-addr routes
show ip mbgp ipv6 neighbors ip-addr routes { best | not-installed-best | unreachable }
show ip mbgp ipv6 neighbors ip-addr routes detail { best | not-installed-best | unreachable }
show ip mbgp ipv6 neighbors ip-addr routes-summary
show ip mbgp ipv6 neighbors last-packet-with-error
show ip mbgp ipv6 neighbors routes-summary
show ip mbgp ipv6 summary

Parameters

neighbors
Specifies a neighbor.

ip-addr
IPv4 address of a neighbor in dotted-decimal notation.

advertised-routes
Specifies the routes that the device has advertised to the neighbor during the current BGP4 session.

detail
Specifies detailed information.

ipv6 address /mask
Specifies an IPv6 address and mask.

flap-statistics
Specifies the route flap statistics for routes received from or sent to a BGP4 neighbor.

last-packet-with-error
Specifies the last packet with an error.

decode
Decodes the last packet that contained an error from any of a device’s neighbors.
received
   Specifies Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

prefix-filter
   Displays the results for ORFs that are prefix-based.

received-routes
   Specifies all route information received in route updates from BGP4 neighbors of the device since the soft-
   reconfiguration feature was enabled.

rib-out-routes
   Displays information about the current BGP4 Routing Information Base (Adj-RIB-Out) for specific neighbors and
   specific destination networks.

routes
   Displays a variety of route information received in UPDATE messages from BGP4 neighbors.

best
   Displays routes received from the neighbor that are the best BGP4 routes to their destination.

not-installed-best
   Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in
   the route table because the device received better routes from other sources.

unreachable
   Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next
   hop.

routes-summary
   Displays all route information received in UPDATE messages from BGP4 neighbors.

summary
   Displays summarized IPv6 unicast information.

Modes
User EXEC mode
show ip multicast
Displays details about the resources used for IP multicast snooping and IGMP snooping entries on all VLANs.

Syntax
```
show ip multicast [ resource | static | vlan vlan-id | A.B.C.D | igmpv3 | pim | static | statistics | tracking]
```

Parameters
- **resource**
  Displays resources used for IP multicast snooping.
- **static**
  Displays configured static IGMP snooping entries in all VLANs.
- **vlan vlan-id**
  Specifies the VLAN.
- **A.B.C.D**
  Specifies the group address to display IP multicast information.
- **igmpv3**
  Displays IGMPv3-specific information.
- **pim**
  Displays PIM-specific information.
- **static**
  Displays configured IGMP snooping entries.
- **statistics**
  Displays IP multicast statistics.
- **tracking**
  Displays IGMPv3 host tracking information.

Modes
- User EXEC mode
- Privileged EXEC mode

Usage Guidelines
You can display IP multicast traffic information in a brief form for all instances or in a detailed form for a specified VLAN or VPLS instance.

Command Output
The `show ip multicast vlan` command displays the following information:
<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Shows the ID of the configured VLAN.</td>
</tr>
<tr>
<td>State</td>
<td>Shows whether the VLAN interface is enabled or disabled.</td>
</tr>
<tr>
<td>Mode</td>
<td>Shows whether the VLAN interface is in active mode or passive mode.</td>
</tr>
<tr>
<td>Active Querier</td>
<td>Shows the active IGMP querier for the VLAN.</td>
</tr>
<tr>
<td>Time Query</td>
<td>Shows the time countdown to generate the next query message.</td>
</tr>
<tr>
<td>(*, G) Count</td>
<td>Shows the count of (*,G) entries.</td>
</tr>
<tr>
<td>(S, G) Count</td>
<td>Shows the count of (S,G) entries.</td>
</tr>
<tr>
<td>Flags</td>
<td>Shows the flags of the outgoing interface.</td>
</tr>
<tr>
<td>V2</td>
<td>V3</td>
</tr>
<tr>
<td>P _G</td>
<td>Indicates that a PIM (*,G) join was received on that interface.</td>
</tr>
<tr>
<td>P _SG</td>
<td>Indicates that a PIM (S,G) join was received on that interface.</td>
</tr>
<tr>
<td>NumOIF</td>
<td>Shows the count of the outgoing interface.</td>
</tr>
<tr>
<td>profile</td>
<td>Shows the profile ID associated with the stream.</td>
</tr>
<tr>
<td>Outgoing Interfaces</td>
<td>Shows the list of outgoing interfaces.</td>
</tr>
<tr>
<td>FID</td>
<td>Shows the FID resource allocated for a particular entry.</td>
</tr>
<tr>
<td>MVID</td>
<td>Shows the MVID resource allocated for a particular entry.</td>
</tr>
</tbody>
</table>

The `show ip multicast vlan vlan-id pim` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Shows the ID of the configured VLAN.</td>
</tr>
<tr>
<td>Group</td>
<td>Shows the IP address of the multicast group.</td>
</tr>
<tr>
<td>Port</td>
<td>Shows the ports attached to the group’s receivers. A port is listed here when it receives a join message for the group, an IGMP membership report for the group, or both.</td>
</tr>
<tr>
<td>Join-Source</td>
<td>Shows the IP address from which a join message was received.</td>
</tr>
<tr>
<td>age</td>
<td>Shows the join-source age.</td>
</tr>
<tr>
<td>Prune-Source</td>
<td>Shows the IP address for pruning a source.</td>
</tr>
<tr>
<td>age</td>
<td>Shows the prune-source age.</td>
</tr>
</tbody>
</table>

Examples

The following example displays the IP multicast resources.

```
device# show ip multicast resource

allocated(U)   in-use(U)   available(U)   allo-fail(U)   up-limit(U)
vlannextn      255          10          245            0         4095
l2mbd          255          1           254            0         2048
portlist       255          2           253            0         8192
v3group        256          0           256            0         8192
v3phyport      1024         0           1024           0          32768
v3source       1024         0           1024           0          32768
v3client       1024         0           1024           0          32768
remote entry   1024         0           1024           0          32768

HW MVID: 0 allocated for L2MCAST of total allocated 0
```
The following example displays the static entries configured on the VLAN.

device# show ip multicast static
Static Entries Configured in VLAN: 2
(*, 230.10.10.10)
Static Uplink: No
Interface Port List: e 2/1

The following example displays the static entries configured on VLAN 2.

device# show ip multicast vlan 2 static
Static Entries Configured in VLAN: 2
(*, 230.10.10.10)
Static Uplink: No
Interface Port List: e 2/1

The following example shows the multicast entries for VLAN 1500.

device# show ip multicast vlan 1500
----------+-----+---------+---------------+-----+-----+------
VLAN     State Mode      Active          Time (*, G)(S, G)
         Querier        Query Count Count
----------+-----+---------+---------------+-----+-----+------
1500     I-Ena Passive  10.25.10.10     103   1     3
----------+-----+---------+---------------+-----+-----+------

Router ports: 7/16 (60s)

Flags-  R: Router Port,  V2|V3: IGMP Receiver,  P_G|P_SG: PIM Join

1   (*, 239.10.10.10) Uptime: 00:01:38   NumOIF: 1   profile: none
   Outgoing Interfaces:
     e7/16 vlan 1500  00:01:38 Flags: ( R [60s] V2 [72s])

1   (10.25.120.131, 239.10.10.10) in e4/1 vlan 1500 Uptime: 00:00:06   NumOIF: 1   profile: none
   Outgoing Interfaces:
     e7/16 vlan 1500  00:00:06 Flags: ( R V2)
     FID: 0xa013     MVID: None

2   (10.25.120.130, 239.10.10.10) in e4/1 vlan 1500 Uptime: 00:00:06   NumOIF: 1   profile: none
   Outgoing Interfaces:
     e7/16 vlan 1500  00:00:06 Flags: ( R V2)
     FID: 0xa012     MVID: None

3   (10.25.120.129, 239.10.10.10) in e4/1 vlan 1500 Uptime: 00:01:39   NumOIF: 1   profile: none
   Outgoing Interfaces:
     e7/16 vlan 1500  00:01:39 Flags: ( R V2)
     FID: 0xa011     MVID: None
The following example displays the PIM SM information for VLAN 2.

device(config)# show ip multicast vlan 2 pim
Number of PIM Groups: 5
Total Number of PIM Entries: 5

<table>
<thead>
<tr>
<th>vlan</th>
<th>group</th>
<th>port</th>
<th>join-source</th>
<th>age</th>
<th>prune-source</th>
<th>age</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>229.0.0.5</td>
<td>1/1</td>
<td>2.1.1.100</td>
<td>180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>229.0.0.4</td>
<td>1/1</td>
<td>2.1.1.100</td>
<td>180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>229.0.0.3</td>
<td>1/1</td>
<td>2.1.1.100</td>
<td>180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>229.0.0.2</td>
<td>1/1</td>
<td>2.1.1.100</td>
<td>180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>229.0.0.1</td>
<td>1/1</td>
<td>2.1.1.100</td>
<td>180</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following example displays the IP multicast statistics for VLAN 1.

device# show ip multicast vlan 1 statistics
IP multicast is enabled - Passive
VLAN ID 1
Reports Received: 34
Leaves Received: 21
General Queries Received: 60
Group Specific Queries Received: 2
Others Received: 0
General Queries Sent: 0
Group Specific Queries Sent: 0

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>The output for the show ip multicast vlan command was modified to include a separate timer for each flag type in a (*, G) entry.</td>
</tr>
</tbody>
</table>
show ip multicast vpls
Displays details about the multicast VPLS instance.

Syntax
show ip multicast vpls vpls-ID

Parameters
vpls-ID
The VPLS ID of the VPLS for which to display the IP multicast PIM information.

Modes
User EXEC mode
Privileged EXEC mode

Command Output
The show ip multicast vpls command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPLS</td>
<td>Shows the ID of the configured VPLS.</td>
</tr>
<tr>
<td>State</td>
<td>Shows whether the VPLS interface is enabled or disabled.</td>
</tr>
<tr>
<td>Mode</td>
<td>Shows whether the VPLS interface is in active mode or passive mode.</td>
</tr>
<tr>
<td>Active Querier</td>
<td>Shows the active IGMP querier for the VPLS.</td>
</tr>
<tr>
<td>Time Query</td>
<td>Shows the time countdown to generate the next query message.</td>
</tr>
<tr>
<td>(*, G) Count</td>
<td>Shows the count of (*,G) entries.</td>
</tr>
<tr>
<td>(S, G) Count</td>
<td>Shows the count of (S,G) entries.</td>
</tr>
<tr>
<td>Router ports</td>
<td>Shows the ports through which the multicast sources can be reached.</td>
</tr>
<tr>
<td>VC Label</td>
<td>Shows the MPLS VC label.</td>
</tr>
<tr>
<td>R Label</td>
<td>Shows the MPLS remote label.</td>
</tr>
<tr>
<td>PIM NBR</td>
<td>Shows the PIM neighbor port.</td>
</tr>
<tr>
<td>Flags</td>
<td>Shows the interface flag for the entry.</td>
</tr>
<tr>
<td>V2</td>
<td>V3</td>
</tr>
<tr>
<td>P_G</td>
<td>Indicates that a PIM (*,G) join was received on that interface.</td>
</tr>
<tr>
<td>P_SG</td>
<td>Indicates that a PIM (S,G) join was received on that interface.</td>
</tr>
<tr>
<td>Mapped MAC Address</td>
<td>Shows the multicast MAC address corresponding to the group.</td>
</tr>
<tr>
<td>NumOIF</td>
<td>Shows the count of the outgoing interface.</td>
</tr>
<tr>
<td>Profile</td>
<td>Shows the profile ID associated with the stream.</td>
</tr>
<tr>
<td>Outgoing Interfaces</td>
<td>Shows the list of outgoing interfaces.</td>
</tr>
<tr>
<td>FID</td>
<td>Shows the FID resource allocated for a particular entry.</td>
</tr>
<tr>
<td>Mapped group address</td>
<td>Shows the mapped group address.</td>
</tr>
<tr>
<td>MVID</td>
<td>Shows the MVID resource allocated for a particular entry.</td>
</tr>
</tbody>
</table>
### Examples

The following example displays detailed IP multicast traffic reduction information for VPLS 1.

```rc
device# show ip multicast vpls 1
----------+-----+---------+---------------+-----+-----+------
VPLS       State Mode      Active          Time (*, G)(S, G)
Querier         Query Count Count
----------+-----+---------+---------------+-----+-----+------
1          Ena   Active    122.122.122.122 7     500   500
----------+-----+---------+---------------+-----+-----+------
Router ports: TNNL peer 122.122.122 (2s) VC Label 983040
Flags-  R: Router Port,  V2|V3: IGMP Receiver,  P_G|P_SG: PIM Join
1    (*, 230.0.0.68) Uptime: 13:04:53     NumOIF: 3       profile: none
Mapped MAC Address: 0100.5e00.0044  FID: 0x0280
Outgoing Interfaces:
    TNNL peer 124.124.124.124 12:48:19 Flags: ( V2 [4s])
e1/10 vlan 200  13:04:45 Flags: ( V3 [2s])
    TNNL peer 122.122.122.122 13:04:53 Flags: ( R [2s] V3 [10s])
1    (200.1.1.100, 230.0.0.68) in e1/11 vlan 200 Uptime: 13:04:53     NumOIF: 3       profile: none
Outgoing Interfaces:
    TNNL peer 124.124.124.124 VC Label 983040 Port e1/5 12:48:19 Flags: ( V2)
e1/10 vlan 200  13:04:45 Flags: ( V3)
    TNNL peer 122.122.122.122 VC Label 983040 Port e1/20 13:04:53 Flags: ( R V3)
FID: 0x0473     MVID:      0
```

The following example displays detailed information about the VPLS instance for IGMPv3.

```rc
device# show ip multicast vpls 1 igmpv3
vlan in-vlan group                port         mode/ag           permit src/age                 deny src
---- ------- -------------------- ------------ ------- ------------------------ ------------------------
200  -       230.0.1.243          1/10         INC              200.1.1.100/205
- -       230.0.1.243              peer 124.124 INC              200.1.1.100/200
200  -       230.0.1.242          1/10         INC              200.1.1.100/205
- -       230.0.1.242              peer 124.124 INC              200.1.1.100/200
200  -       230.0.1.241          1/10         INC              200.1.1.100/205
- -       230.0.1.241              peer 124.124 INC              200.1.1.100/200
200  -       230.0.1.240          1/10         INC              200.1.1.100/205
- -       230.0.1.240              peer 124.124 INC              200.1.1.100/200
200  -       230.0.1.239          1/10         INC              200.1.1.100/205
- -       230.0.1.239              peer 124.124 INC              200.1.1.100/200
200  -       230.0.0.0              1/10         INC              200.1.1.100/205
- -       230.0.0.0                peer 124.124 INC              200.1.1.100/200
```

The following example displays statistics for VPLS 1.

```rc
MLXe8#show ip multicast vpls 1 statistics
VPLS ID 1
Receive stats:                          Transmit stats:
General query           : 0             General query           : 8065
Group specific query     : 0             Group specific query     : 9
IGMP Report             : 15972         IGMP V2 Proxy Sent      : 0
IGMP Leave               : 3              IGMP V3 Proxy Sent      : 0
IGMPV3 Report            : 8005          PIM Proxy Sent          : 0
IGMPV3 Error             : 0              MCT MDUP msg sent       : 0
PIMV2 hello              : 0
PIMV2 join/prune        : 0
PIMV2 J/P pkt error     : 0
MCT MDUP msg recvd      : 0
MCT MDUP msg error      : 0
```
The following example displays VPLS 1 tracking information.

```
<table>
<thead>
<tr>
<th>vlan group</th>
<th>mode/age</th>
<th>permit src/age</th>
<th>client IP/age</th>
</tr>
</thead>
<tbody>
<tr>
<td>230.0.0.0</td>
<td>INC</td>
<td>200.1.1.100/25</td>
<td>200.1.1.40/25</td>
</tr>
</tbody>
</table>
```

MLXe8#show ip multicast vpls 1 pim
Number of PIM Groups: 0
Total Number of PIM Entries: 0

```
<table>
<thead>
<tr>
<th>vlan group</th>
<th>port</th>
<th>join-source</th>
<th>age</th>
<th>prune-source</th>
<th>age</th>
</tr>
</thead>
</table>
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>The output of the command was modified to include a separate timer for each flag type in a (*, G) entry.</td>
</tr>
</tbody>
</table>
show ip ospf

Displays the OSPF state.

Syntax

show ip ospf

Modes

User EXEC mode

Examples

This example displays sample output from the show ip ospf command.

device> show ip ospf

OSPF Version Version 2
Router Id 10.1.1.2
ASBR Status No
ABR Status No (0)
Redistribute Ext Routes from
Initial SPF schedule delay 0 (msecs)
Minimum hold time for SPPs 0 (msecs)
Maximum hold time for SPPs 0 (msecs)
External LSA Counter 0
External LSA Checksum Sum 00000000
Originate New LSA Counter 9
Rx New LSA Counter 6
External LSA Limit 174762
Database Overflow Interval 0
Database Overflow State : NOT OVERFLOWED
RFC 1583 Compatibility : Enabled
Slow neighbor Flap-Action : Disabled, timer 300
Nonstop Routing: Disabled
Graceful Restart: Disabled, timer 120
Graceful Restart Helper: Enabled
LDP-SYNC: Globally enabled, Hold-down time 66 sec
Interfaces with LDP-SYNC enabled:
eth 1/3 eth 1/4
show ip route

Displays information about the routes through LSP tunnels.

Syntax

```
show ip route { ip_addr | num | bgp | connected | import | isis | local | mpls-shortcut | nexthop | ospf | rip | static | summary | tags | vrf }
```

Parameters

- **ip_addr**
  Displays the IP address.

- **num**
  Displays the route table entry whose route number corresponds to the number you specify. For example, if you want to display the tenth row in the table, enter “10”.

- **bgp**
  Displays BGP routes.

- **connected**
  Displays directly connected routes.

- **import**
  Displays imported IPv4 routes.

- **isis**
  Displays IS-IS routes.

- **local**
  Displays local IPv4 routes.

- **mpls-shortcut**
  Displays a list of installed shortcut routes (both LDP and RSVP shortcut routes).

- **nexthop**
  Displays the route next-hop table.

- **ospf**
  Displays OSPF routes.

- **rip**
  Displays RIP routes.

- **static**
  Displays static IP routes.

- **summary**
  Displays a route summary.

- **tags**
  Displays labels associated with routes.
vrf

Displays VRF routes.

Modes

User EXEC mode

Usage Guidelines

Command Output

The `show ip route` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination network of the route.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The next-hop router.</td>
</tr>
<tr>
<td>Port</td>
<td>The port through which the device sends packets to reach the route's destination.</td>
</tr>
<tr>
<td>Cost</td>
<td>The route cost.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The route type, which can be one of the following:</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>The route was ascertained from BGP.</td>
</tr>
<tr>
<td>D</td>
<td>The destination is directly connected to this device.</td>
</tr>
<tr>
<td>R</td>
<td>The route was ascertained from RIP.</td>
</tr>
<tr>
<td>S</td>
<td>The route is a static route.</td>
</tr>
<tr>
<td>*</td>
<td>The route is a candidate default route.</td>
</tr>
<tr>
<td>O</td>
<td>The route is an OSPF route. Unless you use the <code>ospf</code> option to display the route table, <code>O</code> is used for all OSPF routes. If you do not use the <code>ospf</code> option, the following type codes are used:</td>
</tr>
<tr>
<td>O</td>
<td>OSPF intra-area route (within the same area).</td>
</tr>
<tr>
<td>IA</td>
<td>The route is an OSPF inter-area route (a route that passes from one area to another area).</td>
</tr>
<tr>
<td>E1</td>
<td>The route is an OSPF external type 1 route.</td>
</tr>
<tr>
<td>E2</td>
<td>The route is an OSPF external type 2 route.</td>
</tr>
</tbody>
</table>
Examples

The following example displays a sample output of the `show ip route` command.

```
device# show ip route
Total number of IP routes: 1027
Type codes - B:BGP  D:Disconnected  S:Static  R:RIP  O:OSPF; Cost-Dist/Metric

  Destination    Gateway     Port          Cost      Type
  1  10.1.1.1/32    DIRECT      loopback 1    0/0       D
  2  10.1.2.1/32    DIRECT      loopback 2    0/0       D
  3  10.1.3.1/32    DIRECT      loopback 3    0/0       D
  4  10.2.2.2/32    10.0.0.2    eth 1/1       110/10    O
  5  10.3.3.3/32    10.0.0.2    eth 1/1       110/12    O
  6  10.4.4.4/32    10.0.0.2    eth 1/1       110/12    O
  7  10.5.1.5/32    10.5.5.5    lsp( LDP)    200/0     B
  8  10.5.2.5/32    10.5.5.5    lsp( LDP)    200/0     B
  9  10.5.3.5/32    10.0.0.2    eth 1/1       110/13    O
 10  10.5.4.5/32    10.0.0.2    eth 1/1       110/13    O
 11  10.6.1.6/32    10.6.6.6    lsp( LDP)    200/0     B
 12  10.6.2.6/32    10.6.6.6    lsp( LDP)    200/0     B
 13  10.6.3.6/32    10.6.6.6    lsp( LDP)    200/0     B
 14  10.6.4.6/32    10.6.6.6    lsp( LDP)    200/0     B
 15  10.6.5.6/32    10.6.6.6    lsp( LDP)    200/0     B
 16  10.6.6.6/32    10.0.0.2    eth 1/1       110/14    O
 17  10.6.6.6/32    10.8.0.2    eth 1/4       110/14    O
```

The following example displays a sample output of the `show ip route` command using the `mpls-shortcut` option.

```
device# show ip route mpls-shortcut
Type Codes - B:BGP  D:Connected  I:ISIS  O:OSPF  R:RIP  S:Static; Cost - Dist/Metric
  BGP Codes - i:iBGP  e:eBGP
  ISIS Codes - L1:Level-1  L2:Level-2
  OSPF Codes - i:Inter Area  1:External Type 1  2:External Type 2  s:sham link
  STATIC Codes - d:DHCPv6

  Destination    Gateway       Port      Cost   Type  Uptime scr-vrf
  1  10.1.1.1/32    DIRECT      loopback 1    0/0       D
  2  10.1.2.1/32    DIRECT      loopback 2    0/0       D
  3  10.1.3.1/32    DIRECT      loopback 3    0/0       D
  4  10.2.2.2/32    10.0.0.2    eth 1/1       110/10    O
  5  10.3.3.3/32    10.0.0.2    eth 1/1       110/12    O
  6  10.4.4.4/32    10.0.0.2    eth 1/1       110/12    O
  7  10.5.1.5/32    10.5.5.5    lsp( LDP)    200/0     B
  8  10.5.2.5/32    10.5.5.5    lsp( LDP)    200/0     B
  9  10.5.3.5/32    10.0.0.2    eth 1/1       110/13    O
 10  10.5.4.5/32    10.0.0.2    eth 1/1       110/13    O
 11  10.6.1.6/32    10.6.6.6    lsp( LDP)    200/0     B
 12  10.6.2.6/32    10.6.6.6    lsp( LDP)    200/0     B
 13  10.6.3.6/32    10.6.6.6    lsp( LDP)    200/0     B
 14  10.6.4.6/32    10.6.6.6    lsp( LDP)    200/0     B
 15  10.6.5.6/32    10.6.6.6    lsp( LDP)    200/0     B
 16  10.6.6.6/32    10.0.0.2    eth 1/1       110/14    O
 17  10.6.6.6/32    10.8.0.2    eth 1/4       110/14    O
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was modified to include the keyword <code>mpls-shortcut</code>.</td>
</tr>
</tbody>
</table>
show ip static-arp
Displays port, VPLS-ID, VLAN, and VPLS peer information.

Syntax
show ip static-arp [ ip_addr ip_mask ] | num | ethernet slot / port | [ mac-address mac_addr ] | [ vlan vlan_id ] | [ vrf vrf_name ]

Parameters
ip_addr
Specifies the selected IP address.

ip_mask
Specifies the selected IP network mask.

num
Specifies the number of entries to skip.

ethernet slot/port
Displays the specified ethernet port.

mac-address mac_addr
Displays the specified mac address in hexadecimal (xxxx.xxxx.xxxx).

vlan vlan_id
Displays the specified VLAN. A choice of zero (0) signifies

vrf vrf_name
Displays static ARP entries belonging to a given VRF instance.

Modes
EXEC mode

Usage Guidelines

Command Output
The show ip static-arp command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The number of this entry in the table. You specify the entry number when you create the entry.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the device.</td>
</tr>
<tr>
<td>Port/VLAN</td>
<td>Port and VLAN ID.</td>
</tr>
<tr>
<td>ESI</td>
<td>Ethernet Service Instance (ESI) associated with this entry, if any.</td>
</tr>
<tr>
<td>Vpls-Vlan. Port/Vpls-Peer</td>
<td>Shows the VPLS ID under the 'Port' field when applicable. The 'Port' field for the VPLS VE ARP displays in the format ':vpls-vlan; port' or ':vpls-peer_ip_address'</td>
</tr>
</tbody>
</table>
Examples

The following example shows the `show ip static-arp` command output.

```
device(config)# show ip static-arp
Total no. of entries: 2
Index  IP Address   MAC Address     Port/VLAN  ESI  Vpls-Vlan:Port/Vpls-Peer
1      10.10.10.10  0000.0033.4444 100
2      10.11.11.11  0000.0066.7777 4/1
3      10.12.12.12  0000.0023.4343 *:21:3/2
4      10.26.5.12   0000.00F3.4343 *:1.2.3.105
```
**show ip vrrp**

Displays information about IPv4 Virtual Router Redundancy Protocol (VRRP) sessions.

**Syntax**

```
show ip vrrp [ brief ]
show ip vrrp [ ethernet slot|port | ve num ]
show ip vrrp [ statistics [ ethernet slot|port | ve num ] ]
show ip vrrp [ ve num [ vrid VRID ] ]
show ip vrrp [ vrid VRID [ ethernet slot|port | ve num ] ]
```

**Parameters**

- **brief**
  Displays summary information about the VRRP session.
- **ethernet slot port**
  Displays IPv4 VRRP information only for the specified port. A forward slash “/” must be entered between the slot and port variables.
- **statistics**
  Displays statistical information about the VRRP session.
- **ve num**
  Displays IPv4 VRRP information only for the specified virtual Ethernet port.
- **vrid VRID**
  Displays IPv4 VRRP information only for the specified virtual-group ID.

**Modes**

User EXEC mode

**Usage Guidelines**

Use this command to display information about IPv4 VRRP sessions, either in summary or full-detail format. You can also specify a virtual group or interface for which to display output.

This command supports IPv4 VRRP. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

**Command Output**

The `show ip vrrp` command displays the following information.
### Output field Description

| Total number of VRRP routers defined | The total number of virtual routers configured and currently running on this Brocade device. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers. |
| Interface | The interface on which VRRP or VRRP-E is configured. If VRRP or VRRP-E is configured on multiple interfaces, information for each interface is listed separately. |
| VRID | The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row. |
| Current Priority | The current VRRP or VRRP-E priority of this Brocade device for the virtual router. |

#### Flags Codes

- **P**: Preempt
- **2**: V2—VRRP Version 2
- **3**: V3—VRRP Version 3
- **S**: Short-Path-Fwd—Short-path forwarding is enabled

#### State

- **Init**: The virtual router is not enabled (activated). If the state remains Init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other.
  - If the state is Init and the mode is incomplete, make sure that you have specified the IP address for the virtual router.
- **Backup**: This Brocade device is a backup for the virtual router.
- **Master**: This Brocade device is the master for the virtual router.

#### Master IP Address

The IP address of the router interface that is currently the Master for the virtual router. If the IP address is assigned on this device, “Local” is displayed here.

#### Backup IP Address

The IP addresses of the router interfaces that are currently backups for the virtual router. If the IP address is not known in the routing table, “Unknown” is displayed here.

#### Virtual IP Address

The virtual IP address that is being backed up by the virtual router.

---

### Examples

The following example displays VRRP session information in summary format.

```bash
device(config)# show ip vrrp brief

Total number of VRRP routers defined: 2
Flags Codes - P:Preempt 2:V2 3:V3 S:Short-Path-Fwd
Inte- VRID  Current  Flags  State  Master IP  Backup IP  Virtual IP
face    Priority      Address  Address  Address
---------------------------------------------------------------------------
1/1    10    255      P2-  Master  Local  Unknown  10.30.30.2
1/3    13    100      P2-  Master  Local  Unknown  10.13.13.3
device(config)#
```

---
The following example displays IPv4 VRRP configuration information about VRID 1.

device# show ip vrrp vrid 1

Interface 1/1
-------------
auth-type no authentication
VRID 1 (index 1)
interface 1/1
state master
administrative-status enabled
version v2
mode owner
virtual mac aaaa.bbbb.cccc (configured)
priority 255
current priority 255
track-priority 2
hello-interval 1 sec
backup hello-interval 6
show ip vrrp-extended
Displays information about IPv4 Virtual Router Redundancy Protocol Extended (VRRP-E) sessions.

Syntax

```
show ip vrrp-extended [ brief ]
show ip vrrp-extended [ ethernet slot|port | ve num ]
show ip vrrp-extended [ statistics [ ethernet slot|port | ve num ] ]
show ip vrrp-extended [ ve num [ vrid VRID ] ]
show ip vrrp-extended [ vrid VRID [ ethernet slot|port | ve num ] ]
```

Parameters

- brief
  Displays summary information about the VRRP-E session.
- ethernet slot|port
  Displays IPv4 VRRP-E information only for the specified port. A forward slash “/” must be entered between the slot and port variables.
- ve num
  Displays IPv4 VRRP-E information only for the specified virtual Ethernet port.
- statistics
  Displays statistical information about the VRRP-E session.
- vrid VRID
  Displays IPv4 VRRP-E information only for the specified virtual-group ID.

Modes

User EXEC mode

Usage Guidelines

Use this command to display information about IPv4 VRRP-E sessions, either in summary or full-detail format. You can also specify a virtual group or interface for which to display output.

This command supports IPv4 VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

This command can be entered in any mode on the device.

Command Output

The `show ip vrrp-extended` command displays the following information.
### Output Field Description

- **Total number of VRRP-E routers defined**
  - The total number of virtual routers configured and currently running on this Brocade device. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers.

- **Interface**
  - The interface on which VRRP or VRRP-E is configured. If VRRP or VRRP-E is configured on multiple interfaces, information for each interface is listed separately.

- **VRID**
  - The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row.

- **Current Priority**
  - The current VRRP or VRRP-E priority of this Brocade device for the virtual router.

- **Flags**
  - Whether the backup preempt mode is enabled. If the backup preempt mode is enabled, this field contains a "P". If the mode is disabled, this field is blank.
  - **P**: Preempt
  - **2**: V2
  - **3**: V3

- **State**
  - This Brocade device's VRRP state for the virtual router. The state can be one of the following:
    - **Init**: The virtual router is not enabled (activated). If the state remains Init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other.
    - **Backup**: This Brocade device is a backup for the virtual router.
    - **Master**: This Brocade device is the master for the virtual router.

- **Master IP Address**
  - The IP address of the router interface that is currently the Master for the virtual router. If the IP address is assigned on this device, "Local" is displayed here.

- **Backup IP Address**
  - The IP addresses of the router interfaces that are currently backups for the virtual router. If the IP address is not known in the routing table, "Unknown" is displayed here.

- **Virtual IP Address**
  - The virtual IP address that is being backed up by the virtual router.

### Examples

The following example displays summary information for a VRRP-E session.

```
device# show ip vrrp-extended brief

Total number of VRRP-E routers defined: 2
Flags Codes - P:Preempt 2:V2 3:V3 S:Short-Path-Fwd
Interface VRID  Current Priority Flags State Master IP Address Backup IP Address Virtual IP Address
--------------------------------------------------------------
Ve 1  2     255      P2-      Master  Local     10.30.20.2 10.30.30.2
Ve 3  4     100      P2-      Backup  Local     10.30.20.2 10.30.30.2
```
The following example displays the number of configured virtual IPv4 addresses for each VRRP-E router instance and the virtual IPv4 addresses when the VRRP-E multiple virtual IP addresses feature is configured.

device# show ip vrrp-extended brief

Total number of VRRP-Extended routers defined: 3
Flags Codes - P:Preempt 2:V2 3:V3
Short-Path-Fwd Codes - ER: Enabled with revertible option, RT: reverted, NR: not reverted

<table>
<thead>
<tr>
<th>Intf</th>
<th>VRID</th>
<th>Curr Prio</th>
<th>Flags</th>
<th>Master IP</th>
<th>Backup IP (No)</th>
<th>VirtualIP  (7)</th>
<th>Short-Path-Fwd</th>
<th>Track</th>
<th>VPLS-State</th>
<th>MCT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>1</td>
<td>100</td>
<td>P2</td>
<td>Master</td>
<td>Local</td>
<td>(7) 10.10.10.10</td>
<td>Enabled</td>
<td>Disable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.20.20.20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.30.30.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.40.40.40</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.50.50.50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.60.60.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.70.70.70</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following example displays detailed information for a VRRP-E backup device.

device(config)# show ip vrrp-extended

Total number of vrrp-extended routers defined: 1
Interface v10
--------------
auth-type no authentication
VRID 10 (index 1)
interface v10
state backup
administrative-status enabled
mode non-owner(backup)
virtual mac 02e0.52a0.c00a
priority 50
current priority 50
track-priority 5
hello-interval 1 sec
backup hello-interval 60 sec
slow-start timer (configured) 30 sec
advertise backup disabled
dead-interval 3000 ms
preempt-mode true
virtual ip address 10.10.10.254
next hello sent in 1000ms
track-port 1/1 (up)
master router 10.10.10.4 expires in 3.1 sec
short-path-forwarding enabled
The following example displays IPv4 VRRP-E statistics. The "received vrrp-extended packets with unknown or inactive vrid" shows the number of packets that contain virtual router IDs that are not configured on the device or its interface.

device> show ip vrrp-extended statistics

Global VRRP-Extended statistics
-----------------------------
- received vrrp-extended packets with checksum errors = 0
- received vrrp-extended packets with invalid version number = 0
- received vrrp-extended packets with unknown or inactive vrid = 1480

Interface v10
-----------
VRID 1
- number of transitions to backup state = 1
- number of transitions to master state = 1
- total number of vrrp-extended packets received = 0
  . received backup advertisements = 0
  . received packets with zero priority = 0
  . received packets with invalid type = 0
  . received packets with invalid authentication type = 0
  . received packets with authentication type mismatch = 0
  . received packets with authentication failures = 0
  . received packets dropped by owner = 0
  . received packets with ip ttl errors = 0
  . received packets with ip address mismatch = 0
  . received packets with advertisement interval mismatch = 0
  . received packets with invalid length = 0
- total number of vrrp-extended packets sent = 2004
  . sent backup advertisements = 0
  . sent packets with zero priority = 0
- received arp packets dropped = 0
- received proxy arp packets dropped = 0
- received ip packets dropped = 0

The following example displays IPv4 VRRP-E configuration information about VRID 1.

device# show ip vrrp-extended vrid 1

Interface 1/1
-----------
auth-type md5-authentication
VRID 1 (index 1)
  interface 1/1
  state master
  administrative-status disabled
  mode non-owner(backup)
  virtual mac aaaa.bbbb.cccc (configured)
  priority 100
  current priority 100
  track-priority 5
  hello-interval 1 sec
  backup hello-interval 60 sec
  slow-start timer (configured) 30 sec
  advertise backup disabled
  dead-interval 0 ms
  preempt-mode true
  virtual ip address 10.20.1.100
  short-path-forwarding disabled
The following example displays group member information for the VRRP-E scaling feature for VRID 1. Only partial output is displayed.

```
device(config)# show ip vrrp-extended vrid 1
```

VRID 1 (index 1)
interface 1/1
  state master
    administrative-status enabled
  group-member count 3
  group-members
    ethernet 1/2 vrid 2
    ethernet 1/2 vrid 3
    ethernet 1/2 vrid 4

The following example displays group master information for the VRRP-E scaling feature for interface Ethernet 1/1 and VRID 2. Only partial output is displayed.

```
device(config)# show ip vrrp-extended ethernet 1/1 vrid 2
```

VRID 2 (index 2)
interface 1/2
  state master
  administrative-status enabled
  short-path-forwarding disabled
  group-master ethernet 1/1 vrid 1

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was modified to add new output for the VRRP-E scaling using logical groups and VRRP-E multiple virtual IP addresses features.</td>
</tr>
</tbody>
</table>
show ipsec egress-config

Displays egress configuration register contents for IPsec.

Syntax

```
show ipsec egress-config
```

Modes

Privileged EXEC mode

Examples

The following example displays `show ipsec egress-config` command output.

```
device# show ipsec egress-config

IPSec Egress Configuration
Packet with Seq no maxout error: Packet Drop
Packet with NHT entry error: Packet Drop
Packet with unsupported IP header error: Packet Drop
Packet with invalid SPI error: Packet Drop
Non-IP packet for Encapsulation: Packet Drop
Packet encryption: Enabled
IP header check: Enabled
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipsec egress-spi-table

Displays the software copy and the details of the IPsec egress SPI lookup table entry. This command supports IPsec IPv4 and IPv6.

Syntax

    show ipsec egress-spi-table

Modes

    Privileged EXEC mode

Examples

The following example shows the output for an IPsec egress SPI lookup table.

This example is for IPsec IPv4.

    device#show ipsec egress-spi-table
    Egress SPI Lookup Table (total entries: 5)
    idx  spi        spa             dpa             tnnl
    1 0x7883db6f 52.54.112.52    52.54.112.54    112
    2 0xefeaffe5 52.54.111.52    52.54.111.54    111
    device#show ipsec egress-spi-table 2
    egress-spi-id: 2
    SPA: 0x00000000 00000000 00000000 34366f34
    DPA: 0x00000000 00000000 00000000 34366f36
    Mode: IPv4(Tunnel) ReplayCheck: Enabled ESN_Support: Disabled
    TC/TOS: 0(ValidBit: UnSet) HopLimit/TTL: 255
    SPI: 0xeffeaffe5 Salt: 0x88876d98 SequenceNumber: 0x0000000000000002
    ReplayVector: 0x0000000000000001
    AES-256-GCM-KEY: 0x8478313e48f17e2ae1554db2f46762d7865a7a2a51b4760a6e0c6e522e87988

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.9.00</td>
<td>This command was modified to add support for IPsec IPv6.</td>
</tr>
</tbody>
</table>
**show ipsec error-count**

Displays the number of packets encountered with errors, while processing IPsec packets.

**Syntax**

```
show ipsec error-count
```

**Modes**

Privileged EXEC mode

**Examples**

The following example displays `show ipsec error-count` command output.

```
device#show ipsec error-count
  Ingress Replay Error Count : 0
  Ingress Authentication Error Count : 0
  Ingress Pkt Length not in 4byte boundry Error Count : 0
  Ingress Pkt ESP header not in 16byte boundry Error Count : 0
  Ingress Pkt Drop due to Tunnel Mis-match Error Count : 0
  Ingress Pkt EOF before indicated by IP pkt length Error Count : 0
  Ingress Pkt De-encapsulation Error Count : 0
  Ingress Pkt ESP header in fragmented IP pkt Error Count : 0
  Egress Invalid SPI table entry Error Count : 0
  Egress non-IP Pkt Encapsulation Error Count : 0
  Egress Nexthop Table Error Count : 0
  Egress Unsupported Pkt Encapsulation Error Count : 0
  Egress Sequence Number Max-out Error Count : 0
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipsec ingress-config

Displays ingress configuration register contents for IPsec.

Syntax

```
show ipsec ingress-config
```

Modes

Privileged EXEC mode

Examples

The following example displays `show ipsec ingress-config` command output.

device#show ipsec ingress-config

IPSec Ingress Configuration
Packet with encapsulation error: Send to CPU
Packet with tunnel check error: Send to CPU
Packet with replay check error: Send to CPU
Packet with authentication error: Send to CPU
Packet with fragmentation error: Send to CPU
Packet with IP length error: Send to CPU
Hash based on SPI used as Ingress SPI table index
Decapsulation: Enabled
Decryption: Enabled
Next header check: Enabled
IPDA check: Enabled
IPSA check: Enabled
Early EoF check: Enabled
IP length not in 4B boundary check: Disabled
ESP length not in 16B boundary check: Enabled
IP fragmentation check: Enabled
Authentication check: Enabled

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipsec ingress-spi-table

Displays the software copy and the details of the IPsec ingress SPI lookup table entry. This command supports IPsec IPv4 and IPv6.

Syntax

show ipsec ingress-spi-table

Modes

Privileged EXEC mode

Examples

The following example shows the output for an IPsec ingress SPI lookup table.

This example is for IPsec IPv4.

device#show ipsec ingress-spi-table
Ingress SPI Lookup Table (total entries: 5)
idx   spi         spa             dpa             tnnl
 1 0x6e2d9ba8 52.54.112.54 52.54.112.52 112
 2 0x3b191431 52.54.111.54 52.54.111.52 111
device#show ipsec ingress-spi-table 2
      ingress-spi-id: 2
      SPA: 0x00000000 00000000 00000000 34366f36
      DPA: 0x00000000 00000000 00000000 34366f34
      Mode: IPv4(Tunnel)  ReplayCheck: Enabled  ESN_Support: Disabled
      SPI: 0xb191431  Salt: 0xf1db462b  SequenceNumber: 0x0000000000dc042a
      ReplayVector: 0xffffffffffffffff
      AES-256-GCM-KEY: 0xe5649a5cf623dcd134cbf280b9d95eb390719557bd1663d78aece2c6b8eacb0

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.9.00</td>
<td>This command was modified to add support for IPsec IPv6.</td>
</tr>
</tbody>
</table>
show ipsec policy

Displays information about the IP security (IPsec) policy database.

Syntax

```plaintext
show ipsec policy
```

Modes

User EXEC mode

Usage Guidelines

This command may be entered in all configuration modes.

Examples

The following example shows how to display the IPsec policy database.

```plaintext
device# show ipsec policy

IPSEC Security Policy Database(Entries:2)
PType  Dir Proto Source(Prefix:TCP/UDP Port) Destination(Prefix:TCP/UDPPort)
SA: SPDID(vrf:if) Dir Encap SPI Destination
use   in  OSPF  FE80::/10:any ::/0:any
SA: 0:v2           in  ESP   400        FE80::
use   out OSPF  FE80::/10:any ::/0:any
SA: 0:v2           out ESP   400        ::
use   in  all    0.0.0.0/0:any 0.0.0.0/0:any
SA: 1:Tun1         in   ESP  0xBD481319 10.2.10.2
use   out  all 0.0.0.0/0/any 0.0.0.0/0/any
SA: 1:Tun1         out  ESP  0x9EAB77D6 10.2.10.2
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipsec profile
Displays configuration information about IP security (IPsec) profiles.

Syntax
show ipsec profile [profile-name]

Parameters
profile-name
Specifies the name of an IPsec profile.

Modes
User EXEC mode

Usage Guidelines
This command may be entered in all configuration modes.
When an IPsec profile is not specified, this command displays configuration information for all IPsec profiles.

Command Output
The show ipsec profile command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of an IPsec profile.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the IPsec profile.</td>
</tr>
<tr>
<td>Ike Profile</td>
<td>The name of the IKEv2 profile that is attached to this IPsec profile.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The lifetime period (in minutes) for an IPsec SA. The range is from 10 through 1440. The default value is 480 minutes (8 hours). A value of 0 indicates that the IPsec SA remains up indefinitely.</td>
</tr>
<tr>
<td>Anti-replay service</td>
<td>及 Replay window size</td>
</tr>
<tr>
<td>DH group</td>
<td>The Diffie-Hellman group that is used for IKEv2 negotiations.</td>
</tr>
<tr>
<td>Proposal</td>
<td>The name of any IPsec proposals that are attached to this IPsec profile.</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to display IPsec profile configuration information.

device# show ipsec profile

Name: red  Ike Profile: red  Lifetime: 28800
Anti-replay service: Enabled  Replay window size: 64
DH group: None  Proposal: red

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipsec proposal
Displays configuration information about IP security (IPsec) proposals.

Syntax
show ipsec proposal [ proposal-name ]

Parameters
proposal-name
Specifies the name of an IPsec proposal.

Modes
User EXEC mode

Usage Guidelines
This command may be entered in all configuration modes.
When an IPsec proposal is not specified, this command displays configuration information for all IPsec proposals.

Command Output
The show ipsec proposal command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the IPsec proposal.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The transform type.</td>
</tr>
<tr>
<td>Encryption</td>
<td>A list of encryption algorithms that are supported.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The authentication method for data traffic.</td>
</tr>
<tr>
<td>ESN</td>
<td>The Extended Sequence Number (ESN) status.</td>
</tr>
<tr>
<td>Mode</td>
<td>The packet encapsulation mode that is supported.</td>
</tr>
</tbody>
</table>

Examples
The following example shows how to display configuration information for an IPsec proposal named prop_red.

device# show ipsec proposal prop-red

Name : prop_red
Protocol : ESP
Encryption : aes-gcm-256
Authentication: NULL
ESN : Enable
Mode : Tunnel
### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipsec sa
Displays information about the current IPsec Security Associations (SA) that exist on the device or on the IPsec interface. This command supports IPsec IPv4 and IPv6.

Syntax
show ipsec sa [ address [ address | ipv6-address ] | identity id | interface name | peer ip-address ] [ detail ]

Parameters
address address
(Optional) Specifies the IPv4 address of the IPsec interface.

address ipv6-address
(Optional) Specifies the IPv6 address of the IPsec interface.

identity id
(Optional) Specifies the IPsec identity ID value.

interface name
(Optional) Specifies the IPsec interface name.

peer ip-address
(Optional) Specifies the IP address of the IPsec interface.

detail
(Optional) Specifies to include details of the IPsec SA in the output.

Modes
Privileged EXEC mode

Usage Guidelines
If you do not include the optional detail parameter, only the basic information about the IPsec SA is included in the output.

Examples
These examples are for IPsec IPv4.
The following example shows output for command show ipsec sa for the an IPsec SAs on the device.

device# show ipsec sa
IPSEC Security Association Database(Entries:2)
SPID(vrf:if) Dir Encap SPI        Destination
AuthAlg  EncryptAlg Status Mode 
0:v2          out ESP   400        ::
    sha1     Null       ACT    TRAN
0:v2          in  ESP   400        FE80::
    sha1     Null       ACT    TRAN
1:Tun1         in   ESP   0xBD481319   1.2.10.2
    Null      AES-GCM-256 ACT     TNL
1:Tun1         out  ESP   0x9BD481319   1.2.10.2
    Null      AES-GCM-256 ACT     TNL
The following example shows output for command `show ipsec sa <ipaddress> detail` for the IPsec SAs set up on interface 1.2.10.2.

```
device# show ipsec sa address 1.2.10.2 detail
Total ipsec SAs: 2

0:
  interface : tnl 1
  Local address: 1.2.45.1/500, Remote address: 1.2.45.2/500
  Inside vrf: default-vrf
  Local identity (addr/mask/prot/port): address(0.0.0.0/0/0/0)
  Remote identity(addr/mask/prot/port): address(0.0.0.0/0/0/0)
  DF-bit: clear
  Profile-name: red
  DH group: none
  Direction: inbound, SPI: 0x0000004b
  Mode: tunnel,
  ICV size: 16 bytes
  lifetime(sec): Expiring in (4606816/3576)
  Anti-replay service: Enabled, Replay window size: 0
  Status: ACTIVE
  slot Assigned 0
  nht_index 0000ffff
  Is tunnel NHT: false

1:
  interface : tnl 1
  Local address: 1.2.45.1/500, Remote address: 1.2.45.2/500
  Inside vrf: default-vrf
  Local identity (addr/mask/prot/port): address(0.0.0.0/0/0/0)
  Remote identity(addr/mask/prot/port): address(0.0.0.0/0/0/0)
  DF-bit: clear
  Profile-name: red
  DH group: none
  Direction: inbound, SPI: 0x0000009c
  Mode: tunnel,
  ICV size: 16 bytes
  lifetime(k/sec): Expiring in (4606816/3576)
  Anti-replay service: Enabled, Replay window size: 0
  Status: ACTIVE
  slot Assigned 0
  nht_index 00000004
  Is tunnel NHT: true
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.9.00</td>
<td>This command was modified to add support for IPsec IPv6.</td>
</tr>
</tbody>
</table>
**show ipsec statistics**
Displays IPsec Security Association (SA) statistics.

**Syntax**

```bash
show ipsec statistics [tunnel tunnel-id]
```

**Parameters**

- `tunnel tunnel-id`: Specifies the IPsec tunnel ID value.

**Modes**

Privileged EXEC mode

**Command Output**

The `show ipsec statistics` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSecurity Statistics</td>
<td>Displays the total current and total inbound as well as outbound security association statistics.</td>
</tr>
<tr>
<td>IPSecurity Packet Statistics</td>
<td>Displays the total inbound, outbound and dropped packets.</td>
</tr>
<tr>
<td>IPSecurity Error Statistics</td>
<td>Displays the total packet errors, such as the authentication, replay, receive, policy and send errors.</td>
</tr>
</tbody>
</table>

The `show ipsec statistics tunnel` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxPkts</td>
<td>The number of packets received on the interface.</td>
</tr>
<tr>
<td>RxBytes</td>
<td>The volume of data (in bytes) transmitted on the interface.</td>
</tr>
<tr>
<td>TxPkts</td>
<td>The number of packets transmitted by the interface.</td>
</tr>
<tr>
<td>TxBytes</td>
<td>The volume of data (in bytes) transmitted by the interface.</td>
</tr>
<tr>
<td>RxCpPkts</td>
<td>The number of multicast packets received on the interface.</td>
</tr>
<tr>
<td>TxCpPkts</td>
<td>The number of multicast packets transmitted by the interface.</td>
</tr>
</tbody>
</table>
Examples

The following example displays the IPsec SA statistics.

device# show ipsec statistics
IPSecurity Statistics
ipsecEspCurrentInboundSAs 1
ipsecEspCurrentOutboundSA 1
IPSecurity Packet Statistics
ipsecEspTotalInPkts: 0
ipsecEspTotalOutPkts: 7
IPSecurity Error Statistics
ipsecAuthenticationErrors 0
ipsecReplayErrors: 0
ipsecOtherReceiveErrors: 0
ipsecSendErrors: 0
ipsecUnknownSpiErrors: 0

The following example displays the `show ipsec statistics tunnel` command output.

device# show ipsec statistics tunnel
#    Tnnl  RxPkts   RxBytes            TxPkts     TxBytes       RxMcPkts      TxMcPkts
1    1    1393     219574            3696386    510126444       546              321

The following example displays the `show ipsec statistics tunnel` command output for tunnel 1.

device# show ipsec statistics tunnel 1
IPSec tunnel 1 statistics:
RxPkts: 1399
RxBytes: 220522
Multicast Packet Statistics:
RxPkts: 5394

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the <code>show ipsec statistics tunnel</code> command output.</td>
</tr>
</tbody>
</table>
**show ip-tunnels**

Displays information about the configured and valid IPsec tunnels (IPv4 IPsec and IPv6 IPsec) on the device. The information includes the number of the tunnels, source and destination IP addresses, whether tunnels statistics collection is enabled, the protection profile, the spi-idx and more.

**Syntax**

`show ip-tunnels`

**Modes**

Privileged EXEC mode

**Command Output**

The `show ip-tunnels` command displays the following information:

<table>
<thead>
<tr>
<th>This field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 tnnl x UP / DOWN</td>
<td>The status of the interface for manual IPv6 tunnel interface x can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• UP - The tunnel interface is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• DOWN - The tunnel interface is not functioning and is down.</td>
</tr>
<tr>
<td>GRE tnnl x UP or DOWN</td>
<td>The status of the interface for GRE tunnel interface x can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• UP - The tunnel interface is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>• DOWN - The tunnel interface is not functioning and is down.</td>
</tr>
<tr>
<td>GRE Session Enforce</td>
<td>Shows whether the global GRE session enforce feature is enabled. The output is one of the following:</td>
</tr>
<tr>
<td></td>
<td>TRUE - the feature is enabled.</td>
</tr>
<tr>
<td></td>
<td>FALSE - the feature is disabled.</td>
</tr>
<tr>
<td>IPv6 Session Enforce</td>
<td>Shows whether the global IPv6 session enforce feature is enabled. The output is one of the following:</td>
</tr>
<tr>
<td></td>
<td>TRUE - the feature is enabled.</td>
</tr>
<tr>
<td></td>
<td>FALSE - the feature is disabled.</td>
</tr>
<tr>
<td>IP Tunnel Statistics collection</td>
<td>Shows whether the collection of tunnel statistics is enabled. The enable or disable is a global setting that applies to both directions of GRE and manual IPv6 tunnels (unicast and multicast).</td>
</tr>
<tr>
<td>src_ip</td>
<td>The tunnel source can an IPv4 address.</td>
</tr>
<tr>
<td>dst_ip</td>
<td>The tunnel destination can an IPv4 address.</td>
</tr>
<tr>
<td>TTL</td>
<td>The TTL value configured for the outer IP header. The range for TTLs is 1 - 255.</td>
</tr>
<tr>
<td>TOS</td>
<td>The TOS value configured for the outer IP header. The range for TOS values is 1 - 255.</td>
</tr>
<tr>
<td>NHT</td>
<td>The nextHop Table index value.</td>
</tr>
<tr>
<td>MTU</td>
<td>The setting of the IPv6 maximum transmission unit (MTU).</td>
</tr>
</tbody>
</table>
Examples

The following example shows the protection profile and spi-idx for the IPsec tunnels. This example is for IPsec IPv4.

device# show ip-tunnels
# of Configured Tunnels : 1, GRE Session Enforce: FALSE, IPv6 Session Enforce: FALSE,
IP Tunnel Statistics collection Disabled
IPSec IPv4 tnnl 10 UP   : src_ip 1.1.1.1, dst_ip 1.1.1.2
   TTL 255, TOS 0, NHT 1, MTU 1431
   ipsec protection profile : abcd
   egress-spi-idx: 0

device# show ip-tunnels
# of Valid Tunnels : 2, GRE Session Enforce: FALSE, IPv6 Session Enforce: FALSE
IP Tunnel Statistics collection Disabled
IPSec IPv4 tnnl 10 UP : src_ip 1.1.1.1, dst_ip 1.1.1.2, TTL 255, TOS 0
   nht 1, mtu 1431, nht_visited 1, ingresspram_visited 0, arp_index 0x00000001
   PRAM-PFCR2:1: SrcIngressChk 0xffffffff
   ipsec protection profile : abcd
   egress-spi-idx: 1   ingress-spi-idx: 1

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to add support for IPv6.</td>
</tr>
</tbody>
</table>
show ipv6 access-list bindings

Displays all IPv6 access-lists bound to different interfaces. This includes both rule-based ACL and receive access-control list (rACL) information.

Syntax

show ipv6 access-list bindings

Modes

User EXEC node

Usage Guidelines

Examples

The following example displays all IPv6 access-list bindings.

```
device(config)# show ipv6 access-list bindings
!
ipv6 receive access-list b1 sequence 11
ipv6 receive access-list b2 sequence 12
!
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipv6 access-list receive accounting

Displays accounting information for an IPv6 receive access-control list (rACL).

Syntax

    show ipv6 access-list receive accounting { brief | name acl-name }

Parameters

    brief
       Displays IPv6 rACL accounting information in brief.

    name acl-name
       Specifies the name of a receive access-control list.

Modes

User EXEC mode

Examples

The following example displays rACL accounting information for the ACL "b1".

device(config)# show ipv6 access-list receive accounting name b1
IPv6 Receive ACL Accounting Information:
IPv6 Receive ACL b1
ACL hit count for software processing (accum)                    0
HW counters:
    0: permit tcp any host 2000::2
       Hit count: (1 sec)                    0  (1 min)                    0  (5 min)                    0  (accum)                    0
    1: permit udp any host 1000::1
       Hit count: (1 sec)                    0  (1 min)                    0  (5 min)                    0  (accum)                    0

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show ipv6 bgp**
Displays entries in the BGP4+ routing table.

**Syntax**

```plaintext
show ipv6 bgp
show ipv6 bgp ipv6-prefix /prefix-length
show ipv6 bgp ipv6-prefix /prefix-length longer-prefixes
```

**Parameters**

- `ipv6-prefix`
  Specifies an IPv6 network number.

- `/prefix-length`
  Specifies the length of the IPv6 prefix.

- `longer-prefixes`
  Displays routes that match a specified or longer BGP prefix.

**Modes**

User EXEC mode

**Command Output**

The `show ip bgp` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of BGP Routes (appears in display of all BGP routes only)</td>
<td>The number of routes known by the device.</td>
</tr>
<tr>
<td>Number of BGP Routes matching display condition (appears in display that matches specified and longer prefixes)</td>
<td>The number of routes that matched the display parameters you entered. This is the number of routes displayed by the command.</td>
</tr>
<tr>
<td>Status codes</td>
<td>A list of the characters the display uses to indicate the route's status. The status code appears in the left column of the display, to the left of each route. The status codes are described in the command's output.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>A character the display uses to indicate the route's origin. The origin code appears to the right of the AS path (Path field). The origin codes are described in the command's output.</td>
</tr>
<tr>
<td>Network</td>
<td>The network prefix and prefix length.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The next-hop router for reaching the network from the device.</td>
</tr>
<tr>
<td>MED</td>
<td>The value of the route's MED attribute. If the route does not have a metric, this field is blank.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>The degree of preference for this route relative to other routes in the local AS. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.</td>
</tr>
<tr>
<td>Weight</td>
<td>The value that this device associates with routes from a specific neighbor. For example, if the device receives routes to the same destination from two BGP4+ neighbors, the device prefers the route from the neighbor with the larger weight.</td>
</tr>
<tr>
<td>Path</td>
<td>The route's AS path.</td>
</tr>
</tbody>
</table>
Examples

This example displays sample output from the `show ipv6 bgp` command.

```
device# show ipv6 bgp

Total number of BGP Routes: 2
Status codes: s suppressed, d damped, h history, v valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2001:db8::/32</td>
<td>::</td>
<td>1</td>
<td>100</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 2001:db8:1234::/48</td>
<td>::</td>
<td>1</td>
<td>100</td>
<td>32768</td>
<td>?</td>
</tr>
</tbody>
</table>
```

This example displays sample output from the `show ipv6 bgp` command, showing information for prefix 2001:db8::/32, when the `longer-prefixes` keyword is used.

```
device# show ipv6 bgp 2001:db8::/32 longer-prefixes

Number of BGP Routes matching display condition : 3
Status codes: s suppressed, d damped, h history, v valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>MED</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 2001:db8::/32</td>
<td>::</td>
<td>1</td>
<td>100</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 2001:db8:1234::/48</td>
<td>::</td>
<td>1</td>
<td>100</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 2001:db8:e0ff::/48</td>
<td>::</td>
<td>1</td>
<td>100</td>
<td>32768</td>
<td>?</td>
</tr>
</tbody>
</table>

Route is advertised to 1 peers:
2001:db8:4::110(65002)
show ipv6 bgp neighbors
    Displays configuration information and statistics for BGP4+ neighbors of the device.

Syntax
    show ipv6 bgp neighbors
    show ipv6 bgp neighbors ipv6-addr
    show ipv6 bgp neighbors last-packet-with-error
    show ipv6 bgp neighbors routes-summary

Parameters
    ipv6-addr
        IPv6 address of a neighbor in dotted-decimal notation.

    last-packet-with-error
        Displays information about the last packet from a neighbor that contained an error.

    routes-summary
        Displays information about all route information received in UPDATE messages from BGP neighbors.

Modes
    User EXEC mode

Examples
    The following is sample output from the show ipv6 bgp neighbors command.

    device> Total number of BGP Neighbors: 1
        '+': Data in InQueue '->': Data in OutQueue '-' Clearing
        '*': Update Policy 'c': Group change 'p': Group change Pending
        'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

    1   IP Address: 78:2::2, AS: 100 (IBGP), RouterID: 0.0.0.0, VRF: default-vrf
    State: CONNECT, Time: 0h9m7s, KeepAliveTime: 60, HoldTime: 180
    Minimal Route Advertisement Interval: 0 seconds
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
    Sent    : 0       0       0         0            0
    Received: 0       0       0         0            0
    Last Connection Reset Reason:Unknown
    Notification Sent:  Unspecified
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
        Peer configured for IPV6 unicast Routes
    Neighbor ipv6 MPLS Label Capability Negotiation:
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
        ID: 2, Use Count: 2
        BFD:Disabled
    Error: TCP status not available
This example shows sample output from the `show ipv6 bgp neighbors` command.

```
device# show ipv6 bgp neighbors

Total number of BGP Neighbors: 400
's': Data in InQueue '>' : Data in OutQueue '-' : Clearing
'*': Update Policy 'c': Group change 'p': Group change Pending
'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1   IP Address: 105:1::4, AS: 444 (EBGP), RouterID: 4.4.4.4, VRF: default-vrf
    State: ESTABLISHED, Time: 1h7m50s, KeepAliveTime: 60, HoldTime: 180
    KeepAliveTimer Expire in 35 seconds, HoldTimer Expire in 157 seconds
    Minimal Route Advertisement Interval: 0 seconds
    RefreshCapability: Received
    Address Family : IPV6 Unicast
    configured with Add-Path(receive) capability
    Negotiated Add-Path(receive) capability
    Route-map: (out) r
    Messages:  Open Update KeepAlive Notification Refresh-Req
              Sent  1   0     77         0     0
              Received: 1  44    76     0      0
    Last Update Time: NLRI Withdraw NLRI Withdraw
    Tx: ---    Rx: 0h57m34s  ---
    Last Connection Reset Reason: Unknown
    Notification Sent: Unspecified
    Notification Received: Unspecified
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>The command was modified. Description codes were added to display output.</td>
</tr>
<tr>
<td>6.0.0</td>
<td>This command was modified to include BGP add path configuration status.</td>
</tr>
</tbody>
</table>
show ipv6 bgp routes

Displays statistics for the routes in the device’s BGP4+ route table.

Syntax

show ipv6 bgp routes [ num | ipv6-address/prefix | age num | as-path-access-list name | best | cidr-only | community-access-list name | community-reg-expression expression | detail | local | neighbor ipv6-addr | nexthop ipv6-addr | no-best | not-installed-best | prefix-list string | regular-expression name | route-map name | summary | unreachable ]

Parameters

num
Table entry at which the display starts. For example, if you want to list entries beginning with table entry 100, specify 100.

ipv6-address/prefix
Specifies an IPv6 address and prefix.

age num
Displays BGP4+ route information that is filtered by age.

as-path-access-list name
Displays BGP4+ route information that is filtered by autonomous system (AS)-path access control list (ACL).

best
Displays BGP4+ route information that the device selected as best routes.

cidr-only
Displays BGP4+ routes whose network masks do not match their class network length.

community-access-list name
Displays BGP4+ route information for an AS-path community access list.

community-reg-expression expression
Displays BGP4+ route information for an ordered community list regular expression.

detail
Displays BGP4+ detailed route information.

local
Displays BGP4+ route information about selected local routes.

neighbor ipv6-addr
Displays BGP4+ route information about selected BGP neighbors.

nexthop ipv6-addr
Displays BGP4+ route information about routes that are received from the specified next hop.

no-best
Displays BGP4+ route information that the device selected as not best routes.

not-installed-best
Displays BGP4+ route information about best routes that are not installed.
prefix-list string
Displays BGP4+ route information that is filtered by a prefix list.

regular-expression name
Displays BGP4+ route information about routes that are associated with the specified regular expression.

route-map name
Displays BGP4+ route information about routes that use the specified route map.

summary
Displays BGP4+ summary route information.

unreachable
Displays BGP4+ route information about routes whose destinations are unreachable through any of the BGP4+ paths in the BGP route table.

Modes
User EXEC mode

Command Output
The **show ipv6 bgp routes detail** command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of BGP4+ Routes</td>
<td>The number of routes displayed by the command.</td>
</tr>
<tr>
<td>Status codes</td>
<td>A list of the characters the display uses to indicate the route's status. The status code appears in the Status column of the display. The status codes are described in the command's output.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The route's prefix.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>For normal IPv6 routes, next hop is the next hop IPv6 router to reach the destination. For the 6PE routes, next hop is the IPv4-mapped IPv6 address of the peer 6PE router.</td>
</tr>
<tr>
<td>Metric</td>
<td>The value of the route's MED attribute. If the route does not have a metric, this field is blank.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>The degree of preference for the advertised route relative to other routes in the local AS. When the BGP4+ algorithm compares routes on the basis of local preferences, the route with the higher local preference is chosen. The preference can have a value from 0 - 4294967295.</td>
</tr>
<tr>
<td>Weight</td>
<td>The value that this device associates with routes from a specific neighbor. For example, if the receives routes to the same destination from two BGP4+ neighbors, the prefers the route from the neighbor with the larger weight.</td>
</tr>
<tr>
<td>Status</td>
<td>The route's status, which can be one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>A - AGGREGATE. The route is an aggregate route for multiple networks.</td>
</tr>
<tr>
<td></td>
<td>B - BEST. BGP4+ has determined that this is the optimal route to the destination.</td>
</tr>
<tr>
<td></td>
<td>b - NOT-INSTALLED-BEST - BGP4+ has determined that this is the optimal route to the destination but did not install it in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, RIPng, or static IPv6 routes).</td>
</tr>
<tr>
<td></td>
<td>C - CONFED_EBGP. The route was learned from a neighbor in the same confederation and AS, but in a different sub-AS within the confederation.</td>
</tr>
<tr>
<td></td>
<td>D - DAMPED. This route has been dampened (by the route dampening feature), and is currently unusable.</td>
</tr>
<tr>
<td></td>
<td>E - EBGP. The route was learned through a in another AS.</td>
</tr>
</tbody>
</table>
### Output field Description

- **H** - HISTORY. Route dampening is configured for this route, and the route has a history of flapping and is unreachable now.
- **I** - IBGP. The route was learned through an in the same AS.
- **L** - LOCAL. The route originated on this.
- **M** - MULTIPATH. BGP4+ load sharing is enabled and this route was selected as one of the best ones to the destination. The best route among the multiple paths also is marked with “B”.

**NOTE**
If the "m" is shown in lowercase, the software was not able to install the route in the IPv6 route table.

- **S** - SUPPRESSED. This route was suppressed during aggregation and thus is not advertised to neighbors.

<table>
<thead>
<tr>
<th>AS-PATH</th>
<th>The AS-path information for the route.</th>
</tr>
</thead>
</table>

### Examples
The following example shows sample output from the `show ipv6 bgp routes` command.

```
device# show ipv6 bgp routes

Total number of BGP Routes: 4
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
S:SUPPRESSED F:FILTERED s:STALE
Prefix  Next Hop  MED  LocPrf  Weight Status
1 2001:db8:1::/64  2001:db8:1111::2  1  100  32768       BL
AS_PATH:
2 2001:db8:2::/64  2001:db8:30.30.30.1  1  100  0           BI
AS_PATH:
3 2001:db8:1111::/64 ::  0  100  32768       BL
AS_PATH:
4 2001:db8:2222::/64  2001:db8:30.30.30.1  0  100  0           BI
AS_PATH:
```
The following example shows sample output from the `show ipv6 bgp routes` command when the `detail` keyword is used.

```
device# show ipv6 bgp route detail

Total number of BGP Routes: 4
Status A:AGGREGATE B: BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D: DAMPED
S: SUPPRESSED F: FILTERED s: STALE

1 Prefix: 2001:db8:1::/64, Status: BL, Age: 0h1m14s
   NEXT_HOP: 2001:db8:1111::2, Learned from Peer: Local Router
   In-Label: 794624
   LOCAL_PREF: 100, MED: 1, ORIGIN: incomplete, Weight: 32768
   AS PATH:
   Adj_RIB_out count: 1, Admin distance 1

2 Prefix: 2001:db8:2::/64, Status: BI, Age: 0h0m8s
   NEXT_HOP: 2001:db8:ffff:30:1, Learned from Peer: 10.30.30.1 (1)
   Out-Label: 794624
   LOCAL_PREF: 100, MED: 1, ORIGIN: incomplete, Weight: 0
   AS PATH:

3 Prefix: 2001:db8:1111::/64, Status: BL, Age: 0h2m26s
   NEXT_HOP: ::, Learned from Peer: Local Router
   In-Label: 794624
   LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 32768
   AS PATH:
   Adj_RIB_out count: 1, Admin distance 1

4 Prefix: 2001:db8:2222::/64, Status: BI, Age: 0h0m35s
   NEXT_HOP: 2001:db8:ffff:30:1, Learned from Peer: 10.30.30.1 (1)
   Out-Label: 794624
   LOCAL_PREF: 100, MED: 0, ORIGIN: incomplete, Weight: 0
   AS PATH:
```

## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>Command output was modified to include details about BGP additional paths.</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The device’s router ID.</td>
</tr>
<tr>
<td>Local AS Number</td>
<td>The BGP4+ AS number in which the device resides.</td>
</tr>
<tr>
<td>Confederation Identifier</td>
<td>The autonomous system number of the confederation in which the device resides.</td>
</tr>
<tr>
<td>Confederation Peers</td>
<td>The numbers of the local autonomous systems contained in the confederation. This list matches the confederation peer list you configure on the device.</td>
</tr>
<tr>
<td>Maximum Number of Paths Supported for Load Sharing</td>
<td>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.</td>
</tr>
<tr>
<td>Number of Neighbors Configured</td>
<td>The number of BGP4+ neighbors configured on this device.</td>
</tr>
<tr>
<td>Number of Routes Installed</td>
<td>The number of BGP4+ routes in the device’s BGP4+ route table.</td>
</tr>
<tr>
<td>Number of Routes Advertising to All Neighbors</td>
<td>The total of the RtSent and RtToSend columns for all neighbors.</td>
</tr>
<tr>
<td>Number of Attribute Entries Installed</td>
<td>The number of BGP4+ route-attribute entries in the route-attributes table.</td>
</tr>
<tr>
<td>Neighbor Address</td>
<td>The IPv6 addresses of this BGP4+ neighbors.</td>
</tr>
<tr>
<td>AS#</td>
<td>The autonomous system number.</td>
</tr>
</tbody>
</table>
| State                               | The state of this neighbor session with each neighbor. The states are from this perspective of the session, not the neighbor’s perspective. The state values can be one of the following for each:
  - IDLE - The BGP4+ process is waiting to be started. Usually, enabling BGP4+ or establishing a neighbor session starts the BGP4+ process.
    - A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes.
  - ADMND - The neighbor has been administratively shut down.
    - A minus sign (-) indicates that the session has gone down and the software is clearing or removing routes.
  - CONNECT - BGP4+ is waiting for the connection process for the TCP neighbor session to be completed.
  - ACTIVE - BGP4+ is waiting for a TCP connection from the neighbor. |
### Output field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE</td>
</tr>
</tbody>
</table>

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.

### 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<ipv6-address>` command, the TCP receiver queue value will be greater than 0.
- (> -) indicates that there is more BGP data in the outgoing queue.
- (-) - indicates that the session has gone down and the software is clearing or removing routes.
- (*) - indicates that the inbound or outbound policy is being updated for the peer.
- (c) - indicates that the table entry is clearing.
- (p) - indicates that the neighbor ribout group membership change is pending or in progress
- (s) - indicates that the peer has negotiated restart, and the session is in a stale state.
- (r) - indicates that the peer is restarting the BGP4 connection, through restart.
- (^) - on the standby MP indicates that the peer is in the ESTABLISHED state and has received restart capability (in the primary MP).
- (<) - indicates that the device is waiting to receive the "End of RIB" message the peer.

### Time

The time that has passed since the state last changed.

### Accepted

The number of routes received from the neighbor that this installed in the BGP4+ route table. Usually, this number is lower than the RoutesRcvd number. The difference indicates that this filtered out some of the routes received in the UPDATE messages.

### Filtered

The routes or prefixes that have been filtered out.

- If soft reconfiguration is enabled, this field shows how many routes were filtered out (not placed in the BGP4+ route table) but retained in memory.
- If soft reconfiguration is not enabled, this field shows the number of BGP4+ routes that have been filtered out.

### Sent

The number of BGP4+ routes that the has sent to the neighbor.

### ToSend

The number of routes the has queued to send to this neighbor.
Examples

This example displays sample output from the `show ipv6 bgp summary` command.

```
device> show ipv6 bgp summary

BGP4 Summary
Router ID: 10.7.7.7   Local AS Number: 100
Confederation Identifier: not configured
Confederation Peers:
Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
Number of Neighbors Configured: 1, UP: 0
Number of Routes Installed: 0
Number of Routes Advertising to All Neighbors: 0 (0 entries)
Number of Attribute Entries Installed: 0
'+' : Data in InQueue '>' : Data in OutQueue '-' : Clearing
'*' : Update Policy 'c' : Group change 'p' : Group change Pending
'r' : Restarting 's' : Stale '^' : Up before Restart '<' : EOR waiting
Neighbor Address    AS#      State   Time        Rt:Accepted Filtered Sent  ToSend
10:2::2             100      CONN    0h 9m 0s    0           0        0     0     0
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>The command was modified. Description codes were added to display output.</td>
</tr>
</tbody>
</table>
show ipv6 dhcp-relay interface
Displays the IPv6 DHCP relay information for a specific interface.

Syntax
show ipv6 dhcp-relay interface stack/slot/port

Modes
Privileged EXEC mode

Usage Guidelines

Command Output
The show ipv6 dhcp-relay interface command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Relay Information for</td>
<td>The DHCPv6 relay information for the specific interface.</td>
</tr>
<tr>
<td>interface interface-type port-num</td>
<td></td>
</tr>
<tr>
<td>Destination</td>
<td>The configured destination IPv6 address.</td>
</tr>
<tr>
<td>OutgoingInterface</td>
<td>The interface on which the packet will be relayed if the destination relay address is a link local or multicast address.</td>
</tr>
<tr>
<td>Options</td>
<td>The current information about the DHCPv6 relay options for the interface.</td>
</tr>
<tr>
<td>Interface-Id</td>
<td>The interface ID option indicating whether the option is used.</td>
</tr>
<tr>
<td>Client-mac-address</td>
<td>Displays if the client MAC address is used or not.</td>
</tr>
</tbody>
</table>

Examples
The following example displays the DHCPv6 relay information for an interface.

device# show ipv6 dhcp-relay interface ethernet 4/1
DHCPv6 Relay Information for interface eth 4/1:
Destinations:
  Destination          OutgoingInterface
  2000::1               NA
Options:
  Interface-Id: Yes    Remote-Id:Yes    Client-mac-address:Yes
Prefix Delegation Information:
  Current:0 Maximum:8000 AdminDistance:10

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9</td>
<td>This command was modified.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface name.</td>
</tr>
<tr>
<td>Interface-Id</td>
<td>The interface ID option. Yes indicates the option is used. No indicates the option is not used.</td>
</tr>
<tr>
<td>Remote-Id</td>
<td>The remote ID option. Yes indicates the option is used. No indicates the option is not used.</td>
</tr>
<tr>
<td>Client-mac-address</td>
<td>The client MAC address option. Yes or No indicates if the option is used or not.</td>
</tr>
</tbody>
</table>

Examples
The following example displays relay options information.

device# show ipv6 dhcp-relay options
DHCPv6 Relay Options Information:
Interface       Interface-Id     Remote-Id     Client-mac-address
eth 4/1         Yes              Yes           Yes

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9</td>
<td>This command was modified.</td>
</tr>
</tbody>
</table>
**show ipv6 interface tunnel**
Displays the IP addresses and unicast and multicast traffic counters for the specified IPv6 IPsec tunnel. This command cannot be used on IPv4 IPsec tunnels.

**Syntax**
```
show ipv6 interface tunnel num
```

**Parameters**
- `num`
  Specifies the tunnel number.

**Modes**
- User EXEC mode

**Command Output**
The `show interfaces tunnel` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel number</td>
<td>The number of the tunnel.</td>
</tr>
<tr>
<td>Tunnel source</td>
<td>The IP address of the interface that is configured as the source of the tunnel. IP packets are forwarded from this interface across the tunnel.</td>
</tr>
<tr>
<td>Tunnel destination</td>
<td>The IP address of the interface that is configured as the destination of the tunnel. IP packets forwarded from the tunnel source interface are received by this interface.</td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>The specified tunnel mode for the tunnel. This indicates which version of IP (IPv6 or IPv4) has been enabled on the tunnel interface.</td>
</tr>
<tr>
<td>Port name</td>
<td>The specified name of the port. If a name was not specified, the output shows no port name.</td>
</tr>
<tr>
<td>Internet address</td>
<td>The IP address of the port. This is not the IP address of the tunnel source or destination.</td>
</tr>
<tr>
<td>Tunnel TOS</td>
<td>The value to write into the ToS byte in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 99.</td>
</tr>
<tr>
<td>Tunnel TTL</td>
<td>The value to write into the TTL field in the IP header of a tunnel packet (the carrier packet). The value ranges from 0 through 255.</td>
</tr>
<tr>
<td>Tunnel MTU</td>
<td>This maximum size allowable for IP packets entering the tunnel. Packets that exceed the value you specify (or the default) are sent back to the source. The default value is 1480 bytes.</td>
</tr>
<tr>
<td>Tunnel vrf</td>
<td></td>
</tr>
<tr>
<td>Forwarding vrf</td>
<td></td>
</tr>
<tr>
<td>Tunnel protection profile</td>
<td>The name of the IPsec profile used to encapsulate and encrypt the IP packets being transmitted by the tunnel interface. A tunnel profile defines a set of encapsulation and encryption methods used to secure IP packets.</td>
</tr>
<tr>
<td>Tunnel packet statistics</td>
<td>The following packet counts for <em>unicast</em> traffic on the tunnel:</td>
</tr>
</tbody>
</table>
### Output field & Description

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• RxPkts: The total number of IP packets received from the tunnel on the interface.</td>
</tr>
<tr>
<td></td>
<td>• TxPkts: The total number of IP packets transmitted across the tunnel from the interface.</td>
</tr>
<tr>
<td></td>
<td>• RxBytes: The total number of bytes received from the tunnel on the interface. (The total is for IP packets only.)</td>
</tr>
<tr>
<td></td>
<td>• TxBytes: The total number of bytes transmitted across the tunnel from the interface. (The total is for IP packets only.)</td>
</tr>
</tbody>
</table>

### Tunnel multicast packet statistics

The following packet counts for multicast traffic on the tunnel:

- RxMcPkts: The total number of IP multicast packets received from the tunnel on the interface.
- TxMcPkts: The total number of IP multicast packets transmitted across the tunnel from the interface.

### Usage Guidelines

This command is restricted to showing data for IPv6 IPsec tunnels.

**NOTE**

If you want to view the same information for IPv4 IPsec tunnels, use the `show interfaces tunnel` command.

### Examples

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show ipv6 ospf interface
Displays interface information for all or specific OSPFv3-enabled interfaces.

Syntax
show ipv6 ospf interface [ brief ] [ ethernet slot/port ] [ loopback number ] [ tunnel number ] [ ve number ]

Parameters
- **brief**
  Displays brief summary about OSPFv3-enabled interfaces.
- **ethernet**
  Specifies an Ethernet interface
  - **slot**
    Specifies a valid slot number.
  - **port**
    Specifies a valid port number.
- **loopback**
  Specifies a loopback interface.
  - **port-number**
    Specifies the port number for the loopback interface.
- **tunnel**
  Specifies a tunnel.
  - **number**
    Specifies a tunnel number.
- **ve**
  Specifies a virtual Ethernet interface.
  - **vlan_id**
    Specifies the port number for the VE interface.

Modes
User EXEC mode

Usage Guidelines
Use the **brief** keyword to limit the display to the following fields:
- Interface
- Number of Interfaces
- Area
The `show ipv6 ospf interface` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface status</td>
<td>The status of the interface. Possible status includes the following:</td>
</tr>
<tr>
<td>Type</td>
<td>The type of OSPFv3 circuit running on the interface. Possible types include the following:</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address assigned to the interface.</td>
</tr>
<tr>
<td>Instance ID</td>
<td>An identifier for an instance of OSPFv3.</td>
</tr>
<tr>
<td>Router ID</td>
<td>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.</td>
</tr>
<tr>
<td>Area ID</td>
<td>The IPv4 address or numerical value of the area in which the interface belongs.</td>
</tr>
<tr>
<td>Cost</td>
<td>The overhead required to send a packet through the interface.</td>
</tr>
<tr>
<td>default</td>
<td>Shows whether or not the default passive state is set.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the interface. Possible states include the following:</td>
</tr>
</tbody>
</table>

- Up.
- Down.
- BROADCAST
- POINT TO POINT UNKNOWN
- POINT TO POINT
- 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.
<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down -</td>
<td>The interface is unusable. No protocol traffic can be sent or received on such a interface.</td>
</tr>
<tr>
<td>DR other -</td>
<td>The interface is a broadcast or NBMA network on which another router is selected to be the DR.</td>
</tr>
<tr>
<td>Active -</td>
<td>The interface sends or receives all the OSPFv3 control packets, and forms the adjacency.</td>
</tr>
<tr>
<td>Transmit delay</td>
<td>The amount of time, in seconds, it takes to transmit Link State Updates packets on the interface.</td>
</tr>
<tr>
<td>Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Timer intervals</td>
<td>The interval, in seconds, of the hello-interval, dead-interval, and retransmit-interval timers.</td>
</tr>
<tr>
<td>DR</td>
<td>The router ID (IPv4 address) of the DR.</td>
</tr>
<tr>
<td>BDR</td>
<td>The router ID (IPv4 address) of the BDR.</td>
</tr>
<tr>
<td>Number of I/F scoped LSAs</td>
<td>The number of interface LSAs scoped for a specified area, AS, or link.</td>
</tr>
<tr>
<td>DR Election</td>
<td>The number of times the DR election occurred.</td>
</tr>
<tr>
<td>Delayed LSA Ack</td>
<td>The number of the times the interface sent a delayed LSA acknowledgement.</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>The number of neighbors to which the interface is connected.</td>
</tr>
<tr>
<td>Adjacent Neighbor Count</td>
<td>The number of neighbors with which the interface has formed an active adjacency.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>The router ID (IPv4 address) of the neighbor. This field also identifies the neighbor as a DR or BDR, if appropriate.</td>
</tr>
<tr>
<td>Interface statistics</td>
<td>The following statistics are provided for the interface:</td>
</tr>
<tr>
<td>Unknown -</td>
<td>The number of Unknown packets transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received Unknown packets.</td>
</tr>
<tr>
<td>Hello -</td>
<td>The number of Hello packets transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received Hello packets.</td>
</tr>
<tr>
<td>DbDesc -</td>
<td>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.</td>
</tr>
<tr>
<td>LSReq -</td>
<td>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.</td>
</tr>
<tr>
<td>LSUUpdate -</td>
<td>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.</td>
</tr>
<tr>
<td>LSACK -</td>
<td>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.</td>
</tr>
</tbody>
</table>
The `show ipv6 ospf interface brief` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Interfaces</td>
<td>Number of OSPFv3-enabled interfaces.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface type, and the port number or number of the interface.</td>
</tr>
<tr>
<td>Area</td>
<td>The OSPF area configured on the interface.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the link and the protocol. Possible status include the following:</td>
</tr>
<tr>
<td></td>
<td>• Up.</td>
</tr>
<tr>
<td></td>
<td>• Down.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of OSPFv3 circuit running on the interface. Possible types include the following:</td>
</tr>
<tr>
<td></td>
<td>• BCST- Broadcast interface type</td>
</tr>
<tr>
<td></td>
<td>• P2P- Point-to-point interface type</td>
</tr>
<tr>
<td></td>
<td>• UNK- The interface type is not known at this time</td>
</tr>
<tr>
<td>Cost</td>
<td>The overhead required to send a packet across an interface.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the interface. Possible states include the following:</td>
</tr>
<tr>
<td></td>
<td>• DR - The interface is functioning as the Designated Router for OSPFv3.</td>
</tr>
<tr>
<td></td>
<td>• BDR - The interface is functioning as the Backup Designated Router for OSPFv3.</td>
</tr>
<tr>
<td></td>
<td>• Loopback - The interface is functioning as a loopback interface.</td>
</tr>
<tr>
<td></td>
<td>• P2P - The interface is functioning as a point-to-point interface.</td>
</tr>
<tr>
<td></td>
<td>• Passive - The interface is up but it does not take part in forming an adjacency.</td>
</tr>
<tr>
<td></td>
<td>• Waiting - The interface is trying to determine the identity of the BDR for the network.</td>
</tr>
<tr>
<td></td>
<td>• None - The interface does not take part in the OSPF interface state machine.</td>
</tr>
<tr>
<td></td>
<td>• Down - The interface is unusable. No protocol traffic can be sent or received on such an interface.</td>
</tr>
<tr>
<td></td>
<td>• DR other - The interface is a broadcast or NBMA network on which another router is selected to be the DR.</td>
</tr>
<tr>
<td>Nbrs (F/C)</td>
<td>The number of adjacent neighbor routers. The number to the left of the “/” are the neighbor routers that are fully adjacent and the number to the right represents all adjacent neighbor routers.</td>
</tr>
</tbody>
</table>
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
eth 1/3 is down, type BROADCAST
  Interface is disabled
eth 1/8 is up, type BROADCAST
  IPv6 Address: 2001:db8:18:18:18::1/64
  Instance ID 255, Router ID 10.1.1.1
  Area ID 1, Cost 1
  State Active (default passive) DR, Transmit Delay 1 sec, Priority 1
  Timer intervals:
  Hello 10, Hello Jitter 10 Dead 40, Retransmit 5
  Authentication: Enabled
  KeyRolloverTime(sec): Configured: 30 Current: 0
  KeyRolloverState: NotActive
  Outbound: SPI:121212, ESP, SHA1
  Key:1234567890123456789012345678901234567890
  Inbound: SPI:121212, ESP, SHA1
  Key:1234567890123456789012345678901234567890
  DR:10.2.2.2 BDR:10.1.1.1 Number of I/F scoped LSAs is 2
  DRElection: 1 times, DelayedLSAck: 83 times
  Neighbor Count = 1, Adjacent Neighbor Count= 1
  Neighbor:
    10.2.2.2 (DR)
  Statistics of interface eth 1/8:
  Type tx rx tx-byte rx-byte
  Unknown 0 0 0 0
  Hello 1415 1408 56592 56320
  DbDesc 3 3 804 804
  LSReq 1 1 28 28
  LSPUpdate 193 121 15616 9720
  LSAck 85 109 4840 4924
  OSPF messages dropped, no authentication: 0
eth 2/2 is up, type POINT-TO-POINT
  IPv6 Address: 2001:db8:22:22::/64
  Instance ID 0, Router ID 10.1.1.1
  Area ID 100, Cost 1
  State P2P, Transmit Delay 1 sec, Priority 1
  Timer intervals:
  Hello 10, Hello Jitter 10 Dead 40, Retransmit 5
  Authentication: Enabled
  KeyRolloverTime(sec): Configured: 30 Current: 0
  KeyRolloverState: NotActive
  Outbound: SPI:11022, ESP, SHA1
  Key:123456789012345678901234567890
  Inbound: SPI:11022, ESP, SHA1
  Key:123456789012345678901234567890
  DR:0.0.0.0 BDR:0.0.0.0 Number of I/F scoped LSAs is 2
```

This example shows sample output from the `show ipv6 ospf interface brief` command when the `brief` keyword is used.

```
device> show ipv6 ospf interface brief
Number of Interfaces is 3

<table>
<thead>
<tr>
<th>Interface</th>
<th>Area</th>
<th>Status</th>
<th>Type</th>
<th>Cost</th>
<th>State</th>
<th>Nbrs(F/C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth 1/1</td>
<td>1</td>
<td>up</td>
<td>BCST</td>
<td>1</td>
<td>BDR</td>
<td>0/1</td>
</tr>
<tr>
<td>eth 2/1</td>
<td>1</td>
<td>up</td>
<td>BCST</td>
<td>1</td>
<td>DR</td>
<td>0/0</td>
</tr>
<tr>
<td>loopback 1</td>
<td>1</td>
<td>up</td>
<td>BCST</td>
<td>1</td>
<td>Loopback</td>
<td>0/0</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>The <strong>Number of Interfaces</strong> field was added to the <code>show ipv6 ospf interface brief</code> field displays.</td>
</tr>
</tbody>
</table>
show ipv6 vrrp
Displays information about IPv6 Virtual Router Redundancy Protocol (VRRP) sessions.

Syntax

show ipv6 vrrp [ brief ]
show ipv6 vrrp [ ethernet slot|port | ve num ]
show ipv6 vrrp [ statistics [ ethernet slot|port | ve num ] ]
show ipv6 vrrp [ ve num [ vrid VRID] ]
show ipv6 vrrp [ vrid VRID [ ethernet slot|port | ve num ] ]

Parameters

brief
Displays summary information about the IPv6 VRRP session.

ethernet slot port
Displays IPv6 VRRP information only for the specified Ethernet port. A forward slash “/” must be entered between the slot and port variables.

ve num
Displays IPv6 VRRP information only for the specified virtual Ethernet port.

statistics
Displays statistical information about the IPv6 VRRP session.

vrid VRID
Displays IPv6 VRRP information only for the specified virtual router ID (VRID).

Modes
User EXEC mode

Usage Guidelines
This command can be entered in any mode. This command supports IPv6 VRRP; to display information about VRRP Extended (VRRP-E) sessions, use the show ipv6 vrrp-extended command.

Command Output
The following is a partial list of output field descriptions for the show ipv6 vrrp command.

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of VRRP routers defined</td>
<td>The total number of virtual routers configured and currently running on this Brocade device. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface on which VRRP is configured. If VRRP is configured on multiple interfaces, information for each interface is listed separately.</td>
</tr>
</tbody>
</table>
### Output field | Description
--- | ---
VRID | The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row.
state | This Brocade device’s VRRP state for the virtual router. The state can be one of the following:
- **init**—The virtual router is not enabled (activated). If the state remains init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other.
- If the state is init and the mode is incomplete, make sure you have specified the IP address for the virtual router.
- **backup**—This Brocade device is a backup for the virtual router.
- **master**—This Brocade device is the master for the virtual router.
current priority | The current VRRP priority of this Brocade device for the virtual router.
preempt-mode | Whether the backup preempt mode is enabled. If the backup preempt mode is enabled, this field contains a “true.” If the mode is disabled, this field is blank.

### Examples
The following example displays IPv6 VRRP session information in detail.

```
device(config)# show ipv6 vrrp
Total number of VRRP routers defined: 1
Interface 1/3
----------------
auth-type no authentication
VRID 13 (index 2)
interface 1/3
state master
administrative-status enabled
version v3
mode non-owner(backup)
virtual mac 0000.5e00.0217
priority 100
current priority 100
track-priority 1
hello-interval 1000 ms
backup hello-interval 60000 ms
advertise backup disabled
dead-interval 3000 ms
preempt-mode true
ipv6-address 3013::1
next hello sent in 700 ms
short-path-forwarding disabled
```
The following example displays IPv6 VRRP statistical information.

device# show ipv6 vrrp statistics

Global IPv6 VRRP statistics
-----------------------------------
- received vrrp packets with checksum errors = 0
- received vrrp packets with invalid version number = 0
- received vrrp packets with unknown or inactive vrid = 0

Interface 1/3
-------------
VRID 13
- number of transitions to backup state = 1
- number of transitions to master state = 1
- total number of vrrp packets received = 0
  - received backup advertisements = 19
  - received packets with zero priority = 0
  - received packets with invalid type = 0
  - received packets with invalid authentication type = 0
  - received packets with authentication type mismatch = 0
  - received packets with authentication failures = 0
  - received packets dropped by owner = 0
  - received packets with ttl errors = 0
  - received packets with ipv6 address mismatch = 0
  - received packets with advertisement interval mismatch = 0
- total number of vrrp packets sent = 1175
  - sent backup advertisements = 0
  - sent packets with zero priority = 0
- received neighbor solicitation packets dropped = 0
- received proxy neighbor solicitation packets dropped = 0
- received ipv6 packets dropped = 0

The following example displays IPv6 VRRP configuration information about VRID 1.

device# show ipv6 vrrp vrid 1

Interface 1/1
-------------
auth-type no authentication
VRID 1 (index 1)
  interface 1/1
  state master
  administrative-status enabled
  version v3
  mode non-owner (backup)
  virtual mac dddd.eeee.ffff (configured)
  priority 100
  current priority 100
  track-priority 1
  hello-interval 1000 ms
  backup hello-interval 60000 ms
  advertise backup disabled
  dead-interval 3600 ms
  preempt-mode true
  ipv6 address 10:20:1::100
  next hello sent in 400 ms
The following example displays an auto-generated IPv6 virtual link-local address used in the VRRPv3 VRID 1 instance.

**NOTE**
This example is applicable only to the auto-generation of an IPv6 virtual link-local address.

device# show ipv6 vrrp vrid 1
VRID 1 (index 1)
  interface 1/1
  state master
  administrative-status enabled
  version v3
  mode owner
  virtual mac 0000.5e00.0101
  virtual link-local fe80::200:5eff:fe00:201
  priority 255
  current priority 255
  track-priority 2
  hello-interval 1000 ms
  backup hello-interval 60000 ms
  number of configured virtual address 2
  ipv6-address 1:2:45::2
  ipv6-address 1:2:46::2
  next hello sent in 300 ms
  Track MCT-VPLS-State: Disable

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to display an auto-generated IPv6 virtual link-local address.</td>
</tr>
</tbody>
</table>
show ipv6 vrrp-extended
Displays information about IPv6 Virtual Router Redundancy Protocol Extended (VRRP-E) sessions.

Syntax

show ipv6 vrrp-extended [ brief ]
show ipv6 vrrp-extended [ ethernet slot/port | ve num ]
show ipv6 vrrp-extended [ statistics [ ethernet slot/port | ve num ] ]
show ipv6 vrrp-extended [ ve num [ vrid VRID ] ]
show ipv6 vrrp-extended [ vrid VRID | ethernet slot/port | ve num ]

Parameters

brief
Displays summary information about the IPv6 VRRP-E session.

ethernet slot port
Displays IPv6 VRRP-E information only for the specified port.

statistics
Displays statistical information about the IPv6 VRRP-E session.

ve num
Displays IPv6 VRRP-E information only for the specified virtual Ethernet port.

vrid VRID
Displays IPv4 VRRP-E information only for the specified virtual-group ID.

Modes

User EXEC mode

Usage Guidelines

Use this command to display information about IPv6 VRRP-E sessions, either in summary or full-detail format. You can also specify a virtual group or interface for which to display output.

This command supports IPv6 VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Command Output

The show ipv6 vrrp-extended command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of VRRP-E routers defined</td>
<td>The total number of virtual routers configured on this Brocade device.</td>
</tr>
</tbody>
</table>
### Output field | Description
---|---

**NOTE**
The total applies only to the protocol the Brocade device is running. For example, if the Brocade device is running VRRP-E, the total applies only to VRRP-E routers.

| Interface | The interface on which VRRP-E is configured. If VRRP-E is configured on multiple interfaces, information for each interface is listed separately. |
| VRID | The ID of the virtual router configured on this interface. If multiple virtual routers are configured on the interface, information for each virtual router is listed in a separate row. |
| Current Priority | The current VRRP-E priority of this Brocade device for the virtual router. |
| Flags | Whether the backup preempt mode is enabled. If the backup preempt mode is enabled, this field contains a "P". If the mode is disabled, this field is blank. |
| Short-Path-Fwd | This Brocade device’s VRRP state for the virtual router. The state can be one of the following: |

  - **Init**—The virtual router is not enabled (activated). If the state remains Init after you activate the virtual router, make sure that the virtual router is also configured on the other routers and that the routers can communicate with each other.

    **NOTE**
    If the state is Init and the mode is incomplete, make sure you have specified the IP address for the virtual router.

  - **Backup**—This Brocade device is a backup for the virtual router.

  - **Master**—This Brocade device is the master for the virtual router.

| Master IP Address | The IPv6 address of the router interface that is currently the Master for the virtual router. |
| Backup IP Address | The IPv6 addresses of the router interfaces that are currently backups for the virtual router. |
| Virtual IP Address | The virtual IPv6 address that is being backed up by the virtual router. |

### Examples
The following example displays summary information for an IPv6 VRRP-E session.

```
device(config)# show ipv6 vrrp-extended brief
```

**Total number of VRRP routers defined:** 1

<table>
<thead>
<tr>
<th>Flags Codes</th>
<th>P:Preempt 2:V2 3:V3 S:Short-Path-Fwd</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Intf</th>
<th>VRID</th>
<th>CurrPrio</th>
<th>Flags</th>
<th>State</th>
<th>Master-IPv6</th>
<th>Backup-IPv6</th>
<th>Virtual-IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/3</td>
<td>2</td>
<td>100</td>
<td>P3-</td>
<td>Master</td>
<td>Local</td>
<td>3013::2</td>
<td>3013::99</td>
</tr>
</tbody>
</table>
The following example displays detailed IPv6 VRRP-E configuration information about VRID 1.

device# show ipv6 vrrp-extended vrid 1

Interface 1/1/1
----------------
auth-type md5-authentication
VRID 1 (index 1)
interface 1/1/1
state master
administrative-status enabled
mode non-owner(backup)
virtual mac dddd.eeee.ffff (configured)
priority 100
current priority 100
track-priority 5
hello-interval 1 sec
backup hello-interval 60 sec
advertise backup disabled
dead-interval 0 ms
preempt-mode true
virtual ipv6 address 10:20:1::100
device# show ipv6 vrrp-extended vrid 1

Interface 1/1
----------------
auth-type md5-authentication
VRID 1 (index 1)
interface 1/1
state master
administrative-status enabled
mode non-owner(backup)
virtual mac dddd.eeee.ffff (configured)
priority 100
current priority 100
track-priority 5
hello-interval 1 sec
backup hello-interval 60 sec
advertise backup disabled
dead-interval 0 ms
preempt-mode true
virtual ipv6 address 10:20:1::100

device# show ipv6 vrrp-extended vrid 1

The following example displays group member information for the VRRP-E scaling feature for VRID 1. Only partial output is displayed.

device# show ipv6 vrrp-extended ve 100 vrid 1

VRID 2 (index 2)
interface v100
state backup
.
.
.
group-member count 3
group-members
  ve 100 vrid 2
  ve 100 vrid 3
  ve 100 vrid 4
The following example displays group master information for the VRRP-E scaling feature for interface ve 100 and VRID 2. Only partial output is displayed.

```
device# show ipv6 vrrp-extended ve 100 vrid 2
  VRID 2 (index 2)
  interface v100
  state backup
  .
  .
  group-master ve 100 vrid 1
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was modified to add new output for the VRRP-E scaling and VRRP-E multiple IP addresses features.</td>
</tr>
</tbody>
</table>
show isis
  Displays the status of the IS-IS enabled interfaces.

Syntax

Parameters
  config
    Displays integrated IS-IS configuration.
  counts
    Displays integrated IS-IS counters.
  database
    Displays integrated IS-IS database.
    detail
      Displays detailed IS-IS link state database information.
    level1
      Displays IS-IS level-1 link state database.
    level2
      Displays IS-IS level-2 link state database.
  summary
    Displays IS-IS link state database summary.
  hostname
    Displays integrated IS-IS dynamic hostname mapping.
  interface
    Displays integrated IS-IS interface information.
    brief
      Displays IS-IS interface information in brief mode.
  ethernet
    Displays Ethernet port.
  loopback
    Displays loopback interface.
  pos
    Displays POS port.
  tunnel
    Displays tunnel port.
  ve
Displays virtual port.

**ipv6**
Displays IS-IS IPv6 integrated SPF logging.

**spf-log**
Displays integrated IS-IS IPv6 SPF logging.

**neighbor**
Displays integrated IS-IS neighbor list.

**detail**
Displays detailed information.

**routes ip_addr**
Displays integrated IS-IS route by IP address.

**shortcut**
Displays integrated IS-IS shortcut information.

**detail**
Displays IS-IS shortcut detail information.

**lsp**
Displays IS-IS shortcut.

**spf-log**
Displays integrated IS-IS SPF logging.

**detail**
Displays IS-IS SPF log detail information.

**level1**
Displays IS-IS level1 SPF log.

**level2**
Displays IS-IS level 2 SPF log.

**traffic**
Displays IS-IS traffic counts

**Modes**
User EXEC mode

**Usage Guidelines**
Use the **no** form of this command to disable this feature.
This command operates in all modes.

**Command Output**
The **show isis database summary** command shows the following information:
<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of LSPs</td>
<td>Total number of LSPs in database (includes those in the loading state).</td>
</tr>
<tr>
<td>Number of LSPs loading</td>
<td>Number of LSPs pending a full LSP update. This value is non-zero during adjacency formation.</td>
</tr>
<tr>
<td>Number of LSP fragments</td>
<td>The number of LSPs with a non-zero LSP number (a fragment of an LSP).</td>
</tr>
<tr>
<td>Number of Pseudo LSPs</td>
<td>The number of pseudo LSPs.</td>
</tr>
<tr>
<td>Number of Pseudo LSP fragments</td>
<td>The number of pseudo LSPs with a non-zero LSP number (a fragment of an LSP).</td>
</tr>
<tr>
<td>Number of My LSPs</td>
<td>Total number of LSPs originated by this router.</td>
</tr>
<tr>
<td>Number of My LSP fragments</td>
<td>The number of LSPs originated by this router with a non-zero LSP number (a fragment of an LSP).</td>
</tr>
<tr>
<td>Number of My Pseudo LSPs</td>
<td>The number of pseudo LSPs originated by this router.</td>
</tr>
<tr>
<td>Number of My Pseudo LSP fragments</td>
<td>The number of pseudo LSPs originated by this router with a non-zero LSP number (a fragment of an LSP).</td>
</tr>
<tr>
<td>Sum of LSPs Checksum</td>
<td>Total checksum of all LSPs in database (including those in a loading state). This number should be the same across ISIS routers during periods of network stability.</td>
</tr>
</tbody>
</table>

The `show isis shortcut detail` command shows the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the IS-IS shortcut.</td>
</tr>
<tr>
<td>To</td>
<td>This line contains the following information:</td>
</tr>
<tr>
<td></td>
<td>• The LSP endpoint address.</td>
</tr>
<tr>
<td></td>
<td>• Whether or not this LSP is used in the SPF calculation. This field displays either ‘Used by SPF’ or ‘Not used by SPF’.</td>
</tr>
<tr>
<td></td>
<td>• Whether or not the announce metric is used.</td>
</tr>
<tr>
<td>LSP metric</td>
<td>This field displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• The metric value configured at the MPLS LSP configuration level of the CLI.</td>
</tr>
<tr>
<td></td>
<td>• A dash (-), which denotes that the LSP metric is not configured.</td>
</tr>
<tr>
<td></td>
<td>• (Ignored), which denotes that the ignore LSP metric feature is enabled.</td>
</tr>
<tr>
<td>Relative metric</td>
<td>This field displays one of the following:</td>
</tr>
<tr>
<td></td>
<td>• The relative metric value configured with the shortcut IS-IS command.</td>
</tr>
<tr>
<td></td>
<td>• A dash (-), which denoted that the announce metric is not configured.</td>
</tr>
<tr>
<td>Announce metric</td>
<td>This field displays the metric value configured with the shortcut IS-IS command.</td>
</tr>
<tr>
<td>IS-IS System ID</td>
<td>The matching IS-IS system ID for the LSP endpoint.</td>
</tr>
<tr>
<td>Not used by the SPF due to</td>
<td>When the tunnel is not used by SPF, one of the following reasons is noted:</td>
</tr>
<tr>
<td></td>
<td>• Not used by the SPF due to no IS-IS system IS-IS mapping to router-ID. No mapping exists between the tunnel destination and the IS-IS system ID.</td>
</tr>
<tr>
<td></td>
<td>• Not used by the SPF due to IS-IS native route to the LSP tunnel designation. There is no IS-IS native route to the LSP tunnel destination.</td>
</tr>
<tr>
<td></td>
<td>• Not used by SPF due to an IS-IS alternate path preferred to this tunnel. An alternate path has a better metric than the LSP tunnel.</td>
</tr>
<tr>
<td>Not announced due to configuration</td>
<td>Indicates that announce is not configured.</td>
</tr>
<tr>
<td>Last notification from MPLS received</td>
<td>The last time (in hours, minutes, seconds) a status notification was received from MPLS.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the output of the `show isis` command with the default-link-metric configured:

```
device#sh isis
......
Default redistribution metric: 0
Default link metric for level-1: 33
Default link metric for level-2: 5
Protocol Routes redistributed into IS-IS:
......
```

The following example shows the output of the `show isis database summary` command:

```
device# show isis database summary
IS-IS Level-1 Link State Database Summary
Number of LSPs : 2
Number of LSPs loading : 0
Number of LSP fragments : 0
Number of Pseudo LSPs : 1
Number of Pseudo LSP fragments : 0
Number of My LSPs : 1
Number of My LSP fragments : 0
Number of My Pseudo LSPs : 0
Number of My Pseudo LSP fragments : 0
Sum of LSPs Checksum : 0x00018004

IS-IS Level-2 Link State Database Summary
Number of LSPs : 2
Number of LSPs loading : 0
Number of LSP fragments : 0
Number of Pseudo LSPs : 1
Number of My LSPs : 1
Number of My LSP fragments : 0
Number of My Pseudo LSPs : 0
Number of My Pseudo LSP fragments : 0
Sum of LSPs Checksum : 0x00019775
```

Destination addresses: The rows of information below the IP address row are the destinations advertised by the LSP. The Brocade device can reach these destinations by using the IP address listed above as the next hop. Each destination entry contains the following information:

- Metric – The value of the default metric, which is the IS-IS cost of using the IP address above as the next hop to reach this destination.
- Device type – The device type at the destination. The type can be one of the following:
  - End System – The device is an ES.
  - IP-Internal – The device is an ES within the current area. The IP address and subnet mask are listed.
  - IS – The device is another IS. The NET (NSAP address) is listed.
  - IP-Extended – Same as IP-Internal, except the device uses the extended TLV fields described in `draft-ietf-isis-traffic-02.txt` to carry the information.
  - IS-Extended – Same as IS, except the device uses the extended TLV fields described in `draft-ietf-isis-traffic-02.txt` to carry the information.
- Flooding to <num> interface: Identifies the number of interfaces on which the specific LSP entry will be flooded and identifies the interfaces.
- Acking to <num> interface: Identifies the number of interfaces on which the specific LSP entry will be acknowledged and identifies the interfaces.

```
```

TABLE 219 IS-IS detailed LSP database information (Continued)
This field... Displays...

- Number of My Pseudo LSPs : 0
- Number of My Pseudo LSP fragments : 0
- Sum of LSPs Checksum : 0x00019775
The following example shows the output of the `show isis shortcuts` command:

```
device# show isis shortcuts
Configured: 3, Up: 2, Announced: 1
Name        To          Metric          Announce  Tunnel
            (SPF/Announce)             Intf
lsp tomu2   10.4.1.1    10/-            No        tnl1
lsp tomu3   10.3.1.1    -/-             Yes       tnl2
lsp tooolong 10.20.1.1   10/10           Yes       tnl3
toreachmu3
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>A new keyword option <code>ignore-lsp-metric</code> is added to the existing shortcut command under LSP configuration mode.</td>
</tr>
<tr>
<td>5.7.00</td>
<td>The <code>show isis</code> command output is modified to reflect the default-link-metric configured.</td>
</tr>
</tbody>
</table>
show isis shortcut

Displays information about all IS-IS shortcuts configured on the device.

Syntax

```
show isis shortcut [ detail | lsp lsp_name ]
```

Parameters

- `detail`: Displays IS-IS shortcut detail information.
- `lsp lsp_name`: Displays specified LS PIS-IS shortcut.

Modes

User EXEC mode.

Usage Guidelines

Only LSPs that are UP (administratively and operationally enabled in the MPLS domain) are kept in the database and displayed in the show command outputs. LSPs that are down are not kept in the database and are not displayed in the command outputs.

This command also operates in all modes.

Command Output

The `show isis shortcut` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured</td>
<td>The number of IS-IS shortcuts configured.</td>
</tr>
<tr>
<td>Up</td>
<td>The number of IS-IS shortcuts that are UP.</td>
</tr>
<tr>
<td>Announced</td>
<td>The number of IS-IS shortcuts that are advertised.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the IS-IS shortcut. When the name is longer than 11 characters, it wraps to the next line.</td>
</tr>
<tr>
<td>To</td>
<td>The LSP endpoint address.</td>
</tr>
<tr>
<td>Metric (SPF or Announce)</td>
<td>The metric used in the SPF calculation or the metric used in the advertisement of the IS adjacency TLV.</td>
</tr>
</tbody>
</table>

The SPF metric can be one of the following:

- The metric configured at the MPLS LSP configuration level.
- The native IGP metric plus or minus (+ or -) the relative metric configured with the `shortcuts isis` command.
- The native IGP metric
- A dash (-) denotes that the tunnel is not used in SPF calculations.

The Announce metric can be one of the following:

- 10 (the default announce metric)
### Output field | Description
--- | ---
| | • The metric configured with the **announce-metric** keyword
| | • A dash (-) denotes that the tunnel is not used in the IS adjacency TLV advertisement.

#### Announce
Indicates whether or not IS-IS shortcuts are advertised:
- Yes - IS-IS shortcuts are advertised
- No - IS-IS shortcuts are not advertised.

#### Tunnel Intf
The tunnel index of the LSP. This is assigned by MPLS whenever an LSP is created.

---

### Examples

The following example shows the output of the **show isis shortcut** command.

```bash
device# show isis shortcut
Configured: 3, Up: 2, Announced: 1
Name To Metric Announce Tunnel Intf
| SPF/Announce | | |
lsp tomu2 10.4.1.1 10/- No tnl1
lsp tomu3 10.3.1.1 -/- Yes tnl2
lsp tooalong 10.20.1.1 10/10 Yes tnl3
toreachmu3
```

The following example shows the **show isis shortcut detail** command.

```bash
device# show isis shortcut lsp tomu2 detail
lsp tomu2
To 10.1.1.1, Used by SPF (10), Not Announced
LSP metric: 10, Relative metric: -, Announce metric: -
ISIS System Id for 10.4.1.1. is mu2.00-00
Not announced due to configuration
Last notification from MPLS received 0hhm35s ago.
```
show license
Displays general information about all software licenses for all units in a device.

Syntax
show license [ license index ] [ slot number ]

Parameters
license index
Specifies the software license file.

slot slot number
Specifies the slot number of the module. The slot number can be from 1 through 32.

Modes
Privileged EXEC level.

Usage Guidelines
The command can be used to display software licensing information for all available Brocade product families supporting software-based licensing, including node and non-node locked licensing.

Command Output
The show license command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The index number specifies the software license file for a specific stack. The index number is generated by the member unit. The license hash number that uniquely identifies the license.</td>
</tr>
<tr>
<td>Package name</td>
<td>The package name for the license.</td>
</tr>
<tr>
<td>Lid</td>
<td>The license ID. This number is embedded in the Brocade device.</td>
</tr>
<tr>
<td>Slot</td>
<td>Indicates that the license is active in the specified slot for the line card.</td>
</tr>
<tr>
<td>Lid</td>
<td>The license ID. The number is embedded in the Brocade device.</td>
</tr>
<tr>
<td>License Type</td>
<td>Indicates whether the license is normal (permanent) or trial (temporary).</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of the license:</td>
</tr>
<tr>
<td></td>
<td>• Valid - A license is valid if the LID matches the license ID of the device for which the license was purchased, and the package name is recognized by the system.</td>
</tr>
</tbody>
</table>
### Output field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Invalid - The LID does not match the license ID of the device for which the license was purchased.</td>
</tr>
<tr>
<td>• Active - The license is valid and in effect on the device.</td>
</tr>
<tr>
<td>• Not used - The license is not in effect on the device.</td>
</tr>
<tr>
<td>• Expired - For trial licenses only, this indicates that the trial license has expired.</td>
</tr>
</tbody>
</table>

### License Period

If the license type is trial (temporary), this field displays the number of days the license is valid. If the license type is normal (permanent), this field displays Unlimited.

### Trial license information

Indicates the trial license information details as displayed in the `show license` command output.

- days used - The number of days the trial license has been effect.
- hours used - The number of hours the trial license has been in effect.
- days left - The number of days left before the trial license expires.
- hours left - The number of hours left before the trial license expires.

### Examples

The following example output displays information for a Brocade MLXe unit with three licenses installed; the 20x10GbE-X2-Scaling-UPG license, 20x10G-WITH-1G-MODE-ONLY license, and the 20x10G-1G-AND-10G-MODE license.

```
device#show license
Index | Package Name              | Lid           | Slot | License Type | Status | License Period |
1      | 20x10GbE-X2-Scaling-UPG   | dsuFKHJiFKz   | S7   | normal       | active | unlimited      |
2      | 20x10G-WITH-1G-MODE-ONLY  | dsuFKHJiFKz   | S7   | normal       | active | unlimited      |
3      | 20x10G-1G-AND-10G-MODE    | dsuFKHJiFKz   | S7   | normal       | active | unlimited      |
4      | 20x10GbE-X2-Scaling-UPG   | dsuFKHJiFKz   | S19  | normal       | active | unlimited      |
5      | 20x10G-WITH-1G-MODE-ONLY  | dsuFKHJiFKz   | S20  | normal       | active | unlimited      |
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>07.1.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show load-balance mask-options
Displays information about masking options for ECMP and LAG index hash calculations.

Syntax
show load-balance mask-options [ ethernet | gtp | ip | ipv6 | mpls | pbb | slot number ]

Parameters
ethernet
Displays the Ethernet mask options.
gtp
Displays the GPRS Tunneling Protocol (GTP) mask options.
ip
Displays the IPv4 address mask options.
ipv6
Displays the IPv6 address mask options.
mpls
Displays the MPLS mask options.
pbb
Displays the Provider Backbone Bridges (PBB) mask options.
slot number
Displays information about the specified slot number.

Modes
User EXEC mode

Usage Guidelines

Examples
The following example displays information about the Ethernet mask options.

device# show load-balance mask-options ethernet
Mask Ethernet options -
Mask Source MAC is enabled on -
No Slots
Mask Destination MAC is enabled on -
No Slots
Mask Vlan is enabled on -
No Slots
Mask Inner-Vlan is enabled on -
No Slots
Mask ISID is enabled on
The following example displays information about the PBB mask options.

device# show load-balance mask-options pbb
Mask PBB options -
Mask PBB Customer L2 Header is enabled on -
All Slots
Mask PBB Customer IPv4/IPv6 Header is enabled on -
Slot 1
Slot 2 - NPID 1

The following example displays information about the IPv4 address mask options.

device# show load-balance mask-options ip 2
Mask IPv4 options -
    Mask Source address is enabled on -
        No Network Processors
    Mask Destination address is enabled on -
        No Network Processors
    Mask Source address before symmetric lb is enabled on -
        No Network Processors
    Mask Destination address before symmetric lb is enabled on -
        No Network Processors
    Mask Source L4 port is enabled on -
        No Network Processors
    Mask Destination L4 port is enabled on -
        No Network Processors
    Mask Protocol ID is enabled on -
        No Network Processors

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include additional information while displaying the command output.</td>
</tr>
</tbody>
</table>
show macsec ethernet

Displays status information for the designated MACsec interface.

Syntax

    show macsec ethernet slot/port

Parameters

    slot/port
    Interface for which MACsec status information is to be displayed. The interface is designated slot on the device and interface on the slot.

Modes

User EXEC mode

Usage Guidelines

It is recommended that you use the clear macsec ethernet command to clear previous results.

Examples

The following code sample shows details for ethernet interface 1/1.

```
device(config)#show macsec ethernet 1/1
Transmit SC
--------
SC state : Transmitting
SA[0] :
SA state : Transmitting
Next PN  : 94a16300

Receive SC
--------
SCState  : Receiving
SA[0] :
SA State : Receiving
Next FN  : 96a32071
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show macsec statistics ethernet

Displays status information and secure channel statistics for the designated MACsec interface.

Syntax

show macsec statistics ethernet slot / port

Parameters

slot / port

Interface for which MACsec status information is to be displayed. The interface is designated slot on the device and interface on the slot.

Modes

User EXEC mode

Usage Guidelines

It is recommended that you use the clear macsec ethernet command to clear previous results for the show macsec ethernet command before re-executing it.
Examples

The following code sample shows details for ethernet interface 1/1. The interface is verifying MACsec frames and is providing strict replay protection.

Brocade(config)#show macsec statistics ethernet 1/1
Interface statistics
---------------------
rx Untagged Pkts : 3               tx Untagged Pkts : 0
rx Notagged Pkts : 0               tx Too long Pkts : 0
rx Bad Tag Pkts : 0                rx Unknown SCI Pkts : 0
rx No SCI Pkts : 0                 rx Overrun Pkts : 0

Transmit Secure Channels
-------------------------
SC Statistics
Protected Pkts : 0               Protected Octets : 0
Encrypted Pkts : 3               Encrypted Octets : 144

SA[0] Statistics - In use
Protected Pkts : 3               Encrypted Pkts : 3

SA[1] Statistics
Protected Pkts : 0               Encrypted Pkts : 0

Protected Pkts : 0               Encrypted Pkts : 0

Protected Pkts : 0               Encrypted Pkts : 0

Receive Secure Channels
-----------------------
SC Statistics
OK Pkts : 0                     Not Valid Pkts : 0
Unchecked Pkts : 0              Not using SA Pkts : 0
Delayed Pkts : 0                 Unused SA Pkts : 0
Late Pkts : 0                    Validated Octets : 0
Invalid Pkts : 0                 Decrypted Octets : 0

SA[0] Statistics - In use
OK Pkts : 0                     Invalid Pkts : 0
Not using SA Pkts : 0           Unused SA Pkts : 0

SA[1] Statistics
OK Pkts : 0                     Invalid Pkts : 0
Not using SA Pkts : 0           Unused SA Pkts : 0

OK Pkts : 0                     Invalid Pkts : 0
Not using SA Pkts : 0           Unused SA Pkts : 0

OK Pkts : 0                     Invalid Pkts : 0
Not using SA Pkts : 0
Unused SA Pkts : 0

## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show memory histogram
Displays task memory usage information.

**Syntax**

```
show memory histogram [ pool pool-id | below threshold-value | trace taskname ]
```

**Parameters**

- **pool pool-id**
  Specifies the display of memory histogram information for a specific memory pool. The valid range is 0-3, where "0" = OS, "1" = Shared, "2" = Global and "3" = User Private.

- **below threshold-value**
  Specifies the display of memory histogram information when available memory falls below the specified percentage (5, 10 or 20 percent).

- **trace taskname**
  Specifies the display of high CPU condition task traces.

**Modes**

User EXEC mode
Examples

The following example displays memory histogram information.

device# show memory histogram
HISTOGRAM MEMORY SEQUENCE INFO
--------------------------------
DURATION  : 60 s
SEQ IDX   : 1
TIME      : 2012.07.10-11:14:08.539
AVAIL MEM : below 5 %
--------------------------------------------------------
<table>
<thead>
<tr>
<th>POOL</th>
<th>Total Memory (bytes)</th>
<th>Used Memory (bytes)</th>
<th>Available Memory (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>2855272448</td>
<td>2843262976</td>
<td>12009472</td>
</tr>
</tbody>
</table>
--------------------------------------------------------
<table>
<thead>
<tr>
<th>Task Name</th>
<th>Alloc-Number</th>
<th>Alloc-Size(bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>main</td>
<td>1355</td>
<td>28486529</td>
</tr>
<tr>
<td>itc</td>
<td>4</td>
<td>645</td>
</tr>
<tr>
<td>tmr</td>
<td>63</td>
<td>10173</td>
</tr>
<tr>
<td>ip_rx</td>
<td>425</td>
<td>396453</td>
</tr>
<tr>
<td>scp</td>
<td>748</td>
<td>17995881</td>
</tr>
<tr>
<td>lpgent</td>
<td>63</td>
<td>31309</td>
</tr>
<tr>
<td>console</td>
<td>101</td>
<td>3515673</td>
</tr>
<tr>
<td>vlan</td>
<td>44</td>
<td>5814177</td>
</tr>
<tr>
<td>mac_mgr</td>
<td>40</td>
<td>2305485</td>
</tr>
<tr>
<td>mrp</td>
<td>26</td>
<td>8541</td>
</tr>
<tr>
<td>vsrp</td>
<td>28</td>
<td>8557</td>
</tr>
<tr>
<td>erp</td>
<td>28</td>
<td>8557</td>
</tr>
<tr>
<td>mxrp</td>
<td>26</td>
<td>7527</td>
</tr>
<tr>
<td>snms</td>
<td>192</td>
<td>188337</td>
</tr>
<tr>
<td>rtm</td>
<td>98</td>
<td>33724605</td>
</tr>
<tr>
<td>rtm6</td>
<td>109</td>
<td>1918717</td>
</tr>
<tr>
<td>ip_tx</td>
<td>151</td>
<td>1274437</td>
</tr>
<tr>
<td>rip</td>
<td>70</td>
<td>323733</td>
</tr>
<tr>
<td>ospf_msg_task</td>
<td>17</td>
<td>7453</td>
</tr>
<tr>
<td>telnet_0</td>
<td>28</td>
<td>7689</td>
</tr>
<tr>
<td>telnet_1</td>
<td>29</td>
<td>7817</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show metro mp-vlp-queue
Displays priority information about management processor virtual line card (MP-VLP) queues on Brocade NetIron CER Series devices.

Syntax

```shell
show metro mp-vlp-queue
```

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view statistics about messages from the MP are that are queued in the VLP to dequeue.

**NOTE**
If the Dequeue Time is less than 1 millisecond, it is not recorded in the `show metro mp-vlp-queue` statistics. The corresponding timestamp is also not recorded. The initial timestamp is shown as `0000.00.00-00:00:00.000`.

Command Output

The `show metro mp-vlp-queue` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP =&gt; VLP Queue</td>
<td>The queue priority: high, medium, or low.</td>
</tr>
<tr>
<td>Queue Size</td>
<td>The maximum amount of packet counts that the queue can handle at a given time.</td>
</tr>
<tr>
<td>Total Pkt Count</td>
<td>The total count of messages queued in each queue.</td>
</tr>
<tr>
<td>Current Pkt Count</td>
<td>The count of messages queued at a specific moment in each queue.</td>
</tr>
<tr>
<td>Pkt High WM</td>
<td>The maximum messages reached in the queue at any point of time.</td>
</tr>
<tr>
<td>Pkt drop Count</td>
<td>The amount of messages that were dropped because the queue was full.</td>
</tr>
<tr>
<td>Dequeue High WM(msec)</td>
<td>The longest period of time, in milliseconds, that a message remained in that queue.</td>
</tr>
<tr>
<td>Timestamp Pkt High WM(High)</td>
<td>The timestamp for the time when the high water mark for the number of messages in the high priority queue is reached.</td>
</tr>
<tr>
<td>Timestamp Pkt High WM(Medium)</td>
<td>The timestamp for the time when the high water mark for the number of messages in the medium priority queue is reached.</td>
</tr>
<tr>
<td>Timestamp Pkt High WM(Low)</td>
<td>The timestamp for the time when the high water mark for the number of messages in the low priority queue is reached.</td>
</tr>
<tr>
<td>Timestamp Dequeue Time HWM(High)</td>
<td>The timestamp for the time when the most delay is observed in the high priority queue.</td>
</tr>
<tr>
<td>Timestamp Dequeue Time HWM(Medium)</td>
<td>The timestamp for the time when the most delay is observed in the medium priority queue.</td>
</tr>
<tr>
<td>Timestamp Dequeue Time HWM(Low)</td>
<td>The timestamp for the time when the most delay is observed in the low priority queue.</td>
</tr>
</tbody>
</table>
Examples

This example shows sample output from the `show metro mp-vlp-queue` command. Three MP-VLP queues are shown with priority High, Medium and Low. The messages from the MP are queued in these queues for the VLP to dequeue.

LP-1# show metro mp-vlp-queue

<table>
<thead>
<tr>
<th>MP =&gt; VLP Queue</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Pkt Count</td>
<td>2160279</td>
<td>0</td>
<td>61210672</td>
</tr>
<tr>
<td>Current Pkt Count</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pkt High WM</td>
<td>13</td>
<td>0</td>
<td>1992</td>
</tr>
<tr>
<td>Pkt drop count</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dequeue Time HWM(msec)</td>
<td>12000</td>
<td>0</td>
<td>12675</td>
</tr>
</tbody>
</table>

Timestamp Pkt High WM(High) : [13]: 2015.02.25-08:07:16.533
Timestamp Pkt High WM(Medium) : [0]: 0000.00.00-00:00:00.000
Timestamp Pkt High WM(Low) : [1992]: 2015.02.25-08:07:17.223

Timestamp Dequeue Time HWM(High) : [12000]: 2015.02.25-08:07:17.230
Timestamp Dequeue Time HWM(Medium) : [0]: 0000.00.00-00:00:00.000
Timestamp Dequeue Time HWM(Low) : [12675]: 2015.02.25-08:07:17.800

This example shows sample output from the `show metro mp-vlp-queue` command after statistics have been cleared using the `clear metro mp-vlp-queue` command.

LP-1# show metro mp-vlp-queue

<table>
<thead>
<tr>
<th>MP =&gt; VLP Queue</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Pkt Count</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Current Pkt Count</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pkt High WM</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pkt drop count</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dequeue Time HWM(msec)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Timestamp Pkt High WM(High) : [0]: 0000.00.00-00:00:00:00000
Timestamp Pkt High WM(Medium) : [0]: 0000.00.00-00:00:00:00000
Timestamp Pkt High WM(Low) : [0]: 0000.00.00-00:00:00:00000

Timestamp Dequeue Time HWM(High) : [0]: 0000.00.00-00:00:00:00000
Timestamp Dequeue Time HWM(Medium) : [0]: 0000.00.00-00:00:00:00000
Timestamp Dequeue Time HWM(Low) : [0]: 0000.00.00-00:00:00:00000

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring id</td>
<td>The metro ring ID.</td>
</tr>
<tr>
<td>Diag state</td>
<td>The state of ring diagnostics.</td>
</tr>
<tr>
<td>RHP average time</td>
<td>The average round-trip time for an Ring Hello Packet (RHP) packet on the ring. The calculated time has a granularity of 1 microsecond.</td>
</tr>
<tr>
<td>Recommended hello time</td>
<td>The hello time recommended by the software based on the RHP average round-trip time.</td>
</tr>
<tr>
<td>Recommended Prefwing time</td>
<td>The preforwarding time recommended by the software based on the RHP average round-trip time.</td>
</tr>
<tr>
<td>Diag frame sent</td>
<td>The number of diagnostic RHPs sent for the test.</td>
</tr>
<tr>
<td>Diag frame lost</td>
<td>The number of diagnostic RHPs lost during the test.</td>
</tr>
</tbody>
</table>

The `show metro-ring ring-id` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring id</td>
<td>The metro ring ID.</td>
</tr>
<tr>
<td>State</td>
<td>The state of MRP. The state can be enabled or disabled.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ring role</td>
<td>Whether this node is the master for the ring. The role can be master or member.</td>
</tr>
<tr>
<td>Master vlan</td>
<td>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.</td>
</tr>
<tr>
<td>Topo group</td>
<td>The topology group ID.</td>
</tr>
<tr>
<td>Hello time</td>
<td>The interval, in milliseconds, at which the forwarding port on the ring master node sends RHPs.</td>
</tr>
<tr>
<td>Prefwng time</td>
<td>The number of milliseconds an MRP interface that has entered the preforwarding state will wait before changing to the forwarding state.</td>
</tr>
<tr>
<td>Ring interfaces</td>
<td>The ring interfaces in the device. If the interfaces are part of a LAG, only the primary ports of the groups are listed.</td>
</tr>
<tr>
<td>Interface role</td>
<td>The interface role can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• primary</td>
</tr>
<tr>
<td></td>
<td>- Master node - The interface generates RHPs.</td>
</tr>
<tr>
<td></td>
<td>- Member node - The interface forwards RHPs received on the other interface (the secondary interface).</td>
</tr>
<tr>
<td></td>
<td>• secondary - The interface does not generate RHPs.</td>
</tr>
<tr>
<td></td>
<td>- Master node - The interface listens for RHPs.</td>
</tr>
<tr>
<td></td>
<td>- Member node - The interface receives RHPs.</td>
</tr>
<tr>
<td>Forwarding state</td>
<td>Whether MRP forwarding is enabled on the interface. The forwarding state can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• blocking - The interface is blocking Layer 2 data traffic and RHPs.</td>
</tr>
<tr>
<td></td>
<td>• disabled - The interface is down.</td>
</tr>
<tr>
<td></td>
<td>• forwarding - The interface is forwarding Layer 2 data traffic and RHPs.</td>
</tr>
<tr>
<td></td>
<td>• preforwarding - The interface is listening for RHPs but is blocking Layer 2 data traffic.</td>
</tr>
<tr>
<td>Active interface</td>
<td>The physical interfaces that are sending and receiving RHPs. If a port is disabled, its state is shown as &quot;disabled&quot;. If an interface is part of a LAG, the member port which comes up first is listed.</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Shows if the interface is a regular port or a tunnel port.</td>
</tr>
<tr>
<td>RHPs sent</td>
<td>The number of RHPs sent on the interface.</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>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.</td>
</tr>
<tr>
<td>RHPs rcvd</td>
<td>The number of RHPs received on the interface.</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>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.</td>
</tr>
<tr>
<td>TC RHPs rcvd</td>
<td>The number of Topology Change RHPs received on the interface. A Topology Change RHP indicates that the ring topology has changed.</td>
</tr>
</tbody>
</table>
Output field | Description
--- | ---
State changes | The number of MRP interface state changes that have occurred. The state can be one of the states listed in the Forwarding state field.

**Examples**

The following example displays the MRP diagnostics result on the master node.

```
device# show metro-ring 1 diagnostics
Metro Ring 1 - custA
-------------
diagnostics results
Ring       Diag       RHP average     Recommended     Recommended
id         state      time(microsec)  hello time(ms)  Prefwing time(ms)
1          disabled   < 0             100             300

Diag frame sent      Diag frame lost
0                    0
```

The following example displays the output of the `show metro-ring` command.

```
device# show metro-ring 1
Metro Ring 1
-------------
Ring     State     Ring     Master    Topo       Hello      Prefwing
id                 role     vlan      group      time(ms)   time(ms)
2        enabled   member   2         not conf   100        300
Ring interfaces    Interface role     Forwarding state   Active interface  Interface Type
ethernet 1/1/1     primary            disabled           none              Regular
ethernet 1/1/2     secondary          forwarding         ethernet 2        Tunnel
RHPs sent          RHPs rcvd       TC RHPs rcvd     State changes
3                  0                    0                  4
```
show mmrp
    Displays Multiple MAC Registration Protocol (MMRP) information.

Syntax
    show mmrp [ ethernet slot/port [ vlan vlan-id ] ]

Parameters
    ethernet slot port
        Displays information for a specific Ethernet port.

    vlan vlan-id
        Displays information for a specific virtual LAN (VLAN).

Modes
    User EXEC mode

Usage Guidelines
    MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

    Use this command without any options to review MMRP information for all ports and VLANs. Use the optional ethernet and vlan keywords to display specific information about interfaces and VLANs that are registered as MMRP members.

Examples
    The following example shows MMRP information for Ethernet interface 1/1.

    device> show mmrp ethernet 1/1
    ------------------------------------------------------------------
    MMRP Status:           Enabled
    Join-timer(in ms):     500
    Leave-timer(in ms):    1600
    Leaveall-timer(in ms): 10000
    Include-vlan:          100,200,300-500,666
    P2p:                   Yes
    ------------------------------------------------------------------
    Port   Vlan   Mac-count
    ------------------------
    1/1    100    3
    1/1    200    1
The following example shows MMRP information for VLAN 100.

device> show mmrp ethernet 1/1 vlan 100
----------------------------------------------------------
MMRP Status:       Enabled
Join-timer(in ms): 500
Leave-timer(in ms): 1600
Leaveall-timer(in ms): 10000
Include-vlan:      100,200,300-500,666
P2p:              Yes
----------------------------------------------------------
Port  Vlan  Mac-count
-------  ----  ---------
1/1     100   3
show mmrp attributes
Displays Multiple MAC Registration Protocol (MMRP) attributes.

Syntax
show mmrp attributes [ ethernet slot/port [ vlan vlan-id ] ]

Parameters
ethernet slot port
Displays information for a specific Ethernet port.

vlan vlan-id
Displays information for a specific virtual LAN (VLAN).

Modes
User EXEC mode

Usage Guidelines
MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

Use this command to review the addresses that are attached to various ports (and optionally, VLANs) and determine the registration state and applicant status. If no keyword options are used, information about all interfaces and VLANs that are registered as MMRP members is displayed.

Examples
The following example displays the MMRP registered member states.

device> show mmrp attributes

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>Mac-address</th>
<th>Registrar</th>
<th>Registrar</th>
<th>Applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>State</td>
<td>Mgmt</td>
<td>State</td>
</tr>
<tr>
<td>1/1</td>
<td>100</td>
<td>011e.8300.3001</td>
<td>IN</td>
<td>Fixed</td>
<td>Quiet</td>
</tr>
<tr>
<td>1/5</td>
<td>100</td>
<td>011e.8300.3001</td>
<td>LV</td>
<td>Normal</td>
<td>Quiet</td>
</tr>
<tr>
<td>1/5</td>
<td>100</td>
<td>011e.8300.3001</td>
<td>MT</td>
<td>Normal</td>
<td>Quiet</td>
</tr>
<tr>
<td>1/1</td>
<td>200</td>
<td>011e.8300.3002</td>
<td>IN</td>
<td>Fixed</td>
<td>Quiet</td>
</tr>
</tbody>
</table>

The following example displays the MMRP information for Ethernet interface 1/1.

device> show mmrp attributes ethernet 1/1

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>Mac-address</th>
<th>Registrar</th>
<th>Registrar</th>
<th>Applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>State</td>
<td>Mgmt</td>
<td>State</td>
</tr>
<tr>
<td>1/1</td>
<td>100</td>
<td>011e.8300.3001</td>
<td>IN</td>
<td>Fixed</td>
<td>Quiet</td>
</tr>
<tr>
<td>1/1</td>
<td>200</td>
<td>011e.8300.3002</td>
<td>IN</td>
<td>Fixed</td>
<td>Quiet</td>
</tr>
</tbody>
</table>
The following example displays the MMRP information for VLAN 100.

device> show mmrp attributes ethernet 1/1 vlan 100

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>Mac-address</th>
<th>Registrar State</th>
<th>Registrar Mgmt</th>
<th>Applicant State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>100</td>
<td>011e.8300.3001</td>
<td>IN</td>
<td>Fixed</td>
<td>Quiet Active</td>
</tr>
</tbody>
</table>
show mmrp config
Displays the Multiple MAC Registration Protocol (MMRP) configuration.

Syntax
show mmrp config

Modes
User EXEC mode

Usage Guidelines
MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

Use this command to review the MMRP parameters configured on this device.

Examples
The following example displays the parameters configured for MMRP on this device.

device> show mmrp config

mmrp enable
  mmrp include-vlan 100,200,300
  mmrp timer join 400 leave 1400 leave-all 10000

interface ethernet 1/1
  mmrp enable
  mmrp point-to-point
  mmrp timer join 500 leave 2000 leave-all 15000
  mmrp include-vlan 600,500,300
  enable

interface ethernet 1/3
  mmrp enable
  mmrp timer join 600 leave 2200 leave-all 20000
  enable

interface ethernet 1/5
  mmrp enable
  mmrp point-to-point
  mmrp timer join 500 leave 2000 leave-all 15000
  enable
**show mmrp statistics**

Displays Multiple MAC Registration Protocol (MMRP) statistics.

**Syntax**

```
show mmrp statistics [vlan vlan-id]
```

**Parameters**

- `vlan vlan-id`
  
  Displays information for a specific virtual LAN (VLAN).

**Modes**

- User EXEC mode

**Usage Guidelines**

MMRP provides a mechanism for end-stations and bridges to dynamically register or declare group membership for individual MAC addresses to bridges attached in the same LAN or VLAN.

Use this command to review the statistics for MMRP members. If the `vlan` keyword option is used, statistics for the specified VLAN are displayed.

**Examples**

The following example displays all MMRP statistics for this device.

```
device> show mmrp statistics

Vlan 100 - Ports 1/1 to 1/5
-------------------------------------
Message type   Received   Transmitted
-------------------------------------
In              0          0
Join In         0          0
Join Empty      0          0
Empty           0          156
Leave           0          0
Leave All       40         41
-------------------------------------
Total PDUs      2          826
-------------------------------------

Vlan 200 - Ports 2/1 to 2/5
-------------------------------------
Message type   Received   Transmitted
-------------------------------------
In              0          0
Join In         0          0
Join Empty      0          0
Empty           0          156
Leave           0          0
Leave All       40         41
-------------------------------------
Total PDUs      2          826
-------------------------------------
```
The following example displays MMRP statistics only for VLAN 100.

device> show mmrp statistics vlan 100

Vlan 100 - Ports 1/1 to 1/6

<table>
<thead>
<tr>
<th>Message type</th>
<th>Received</th>
<th>Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>In</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Join In</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Join Empty</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Empty</td>
<td>0</td>
<td>156</td>
</tr>
<tr>
<td>Leave</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Leave All</td>
<td>40</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>826</td>
</tr>
</tbody>
</table>

Show Commands
show mpls autobw-threshold-table

Displays the global-threshold table.

Syntax

show mpls autobw-threshold-table

Modes

User EXEC mode

Usage Guidelines

This command displays the global-threshold table with the range of current-bandwidth and the corresponding absolute adjustment-threshold.

This command operates in all modes.

Command Output

The show mpls autobw-threshold table command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range (kbps)</td>
<td>Auto-bandwidth range in kilobytes per second.</td>
</tr>
<tr>
<td>Threshold (kbps)</td>
<td>Auto-bandwidth threshold in kilobytes per second.</td>
</tr>
</tbody>
</table>

Examples

The following example shows the show mpls autobw-threshold-table command.

device# show mpls autobw-threshold-table
Auto-bandwidth threshold table
Range (kbps)     Threshold (kbps)
0-10             2000
11-1000          3000
1001-10000       5000
10001-max        10000

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
show mpls bypass-lsp
Displays all dynamic bypass LSPs along with static bypass LSPs.

Syntax

show mpls bypass-lsp [ brief | wide | detail | name lsp_name extensive [ descending ] | invalid-tunnel-interface
show mpls bypass-lsp { up | down } { detail | extensive [ descending ] | wide }
show mpls bypass-lsp { dynamic | static } { brief | detail | extensive [ descending ] | interface { ethernet slot / port { brief | wide } | pos slot / port { brief | wide } | ve ve-id { brief | wide } )

Parameters

brief
Displays brief information.
detail
Displays detailed information.
wide
Displays long LSP names.
name
Displays LSP by name.
lsp_name
Selected LSP to display.
extensive
Displays detailed information with History.
descending
Displays detailed information with History in reverse chronological order.
invalid-tunnel-interface
Displays LSPs with an invalid tunnel-interface.
up
Displays operationally UP LSPs.
down
Displays operationally DOWN LSPs.
detail
Displays operationally UP/DOWN LSP detailed information.
extensive
Displays operationally UP/DOWN LSP detailed information with History.
descending
Displays operationally UP/DOWN LSPs History in reverse chronological order.
wide
Displays operationally UP/DOWN LSP long names.

dynamic
Displays dynamic bypass LSPs.

static
Displays static bypass LSPs.

brief
Displays dynamic/static LSP brief information.

detail
Displays dynamic/static LSP detailed information

extensive
Displays dynamic/static LSP detailed information with History.

descending
Displays detailed information with History in reverse chronological order.

interface
Displays dynamic/static LSP protected interface.

ethernet slot / port
Specifies an ethernet port.

pos slot / port
Specifies a POS port.

ve ve-id
Specifies a virtual interface (VE).

Modes
User EXEC mode

Examples
The following example displays the command with the brief option.

device# show mpls bypass-lsp dynamic brief
Note: LSPs marked with + are Dynamic Bypass LSPs

<table>
<thead>
<tr>
<th>Name</th>
<th>To</th>
<th>Admin Oper</th>
<th>Tunnel</th>
<th>Up/Dn Retry</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>blsp01</td>
<td>22.22.22.22</td>
<td>UP</td>
<td>UP+</td>
<td>tnl1</td>
<td>1</td>
</tr>
</tbody>
</table>

_2
The following example displays that the non-brief versions include the tunnel-interface index.

```
device#show mpls bypass detail
LSP byp1, to 3.3.3.3, Tunnel interface index: 5002
 From: 120.120.120.2, admin: UP, status: DOWN (CSPP fails: Excluded MPLS interface is down)
Times primary LSP goes up since enabled: 0
 Maximum retries: NONE, no. of retries: 0
 Pri. path: NONE, up: no, active: no
 Setup priority: 7, hold priority: 0
 Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
 CSPP-computation-mode configured: use te-metric(global)
 Constraint-based routing enabled: yes
 Path calculated using constraint-based routing: no
 Path calculated using interface constraint: no
 Path cspp-group computation-mode: disabled, cost: 0
 Tie breaking: random, hop limit: 0
 Exclude interface(s): e3/1
 Active Path attributes:
 Tunnel index: 65535
```

The following example displays information about the specified bypass-lsp using the `show mpls bypass-lsp name name` command.

```
device# show mpls bypass-lsp name t100
LSP t100, to 10.1.1.1
 From: 10.2.2.2, admin: UP, status: UP
Times primary LSP goes up since enabled: 1
 Metric: 0, number of installed aliases: 0   Adaptive
 Maximum retries: NONE, no. of retries: 0
 Pri. path: NONE, up: no, active: no
 Setup priority: 7, hold priority: 0 ReoptimizeTimer: 300
 Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
 Constraint-based routing enabled: yes
 Path calculated using constraint-based routing: no
 Path calculated using interface constraint: no
 Tie breaking: random, hop limit: 0
 Active Path attributes:
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was modified to include filtering based of static bypass types, dynamic bypass types, and protected interface.</td>
</tr>
<tr>
<td>5.6.00</td>
<td>This command was modified to display the cspp-computation mode for the LSP at the local level. This is applicable to bypass LSPs, as well as dynamic bypass LSPs.</td>
</tr>
<tr>
<td>5.8.00</td>
<td>This command was modified to include the <code>descending</code> keyword.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the tunnel-interface index in the display output for all non-brief versions.</td>
</tr>
</tbody>
</table>
show mpls config
Displays user-configured MPLS parameters.

Syntax
show mpls config autobw-template autobw_template_name | autobw-threshold-table | brief | cspf-group cspf_group_name |
dynamic-bypass | lsp lsp_name | path path_name | rsvp | static-lsp transit | vll vll_name | vll-local vll_local_name | vpls vpls_name
show mpls config vpls [ vpls_id | vpls_name ]
show mpls config interface [ ethernet slot/port | pos slot/port | tunnel tunnel_id | ve num ]
show mpls config use-bypass-liberal

Parameters
autobw-template autobw_template_name
Displays the named automatic bandwidth template configuration information.

autobw-threshold-table
Displays autobw-threshold-table.

brief
Displays brief MPLS configuration information.

cspf-group cspf_group_name
Displays the named cspf-group configuration information.

dynamic-bypass dynamic_bypass_name
Displays the named dynamic bypass configuration information.

interface
Displays interface MPLS configuration information.

ethernet slot/port
Display the named ethernet port information.

pos slot/port
Displays the named POS port information.

tunnel tunnel_id
Displays the named tunnel interface information.

ve num
Displays the named virtual ethernet (VE) interface information.

lsp lsp_name
Displays the named LSP configuration information.

path path_name
Displays the named MPLS path configuration information.

rsvp
Displays all RSVP global configurations.

**static-lsp** static\_lsp\_name
Displays the named MPLS static LSPs configuration information.

**use-bypass-liberal**
Displays liberal mode as part of the command.

**vll** vll\_name
Displays the named VLL configuration information.

**vll-local** vll\_local\_name
Displays the named VLL-local configuration information.

**vpls** vpls\_name
Displays the named VPLS configuration information.

**Modes**
Privileged EXEC mode

**Usage Guidelines**
Use the `show mpls config` with the optional `brief` keyword to display the prefix list configuration, instead of the ACL.

This command displays the MPLS configuration that exists for each of the keyword/variable options.

The `show mpls config use-bypass-liberal` command operates under the MPLS router mode (config-mpls-policy).

**Examples**
The following example shows the `show mpls config brief` command.

```
device show mpls config
device(config t)>
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)#
device(config-mpls-policy)# ingress-tunnel-accounting
device(config-mpls-policy)# auto-bandwidth sample-interval 300
device(config-mpls-policy)# idp
device(config-mpls-ldp)# advertise-fec list-abc
```

The following example shows the output was modified to the overload bit configuration.

```
device# show mpls config
device(config t)>
device(config)# router mpls
device(config-mpls)# policy
device(config-mpls-policy)# traffic-eng isis level-1
device(config-mpls-policy)# handle-isis-neighbor-down
device(config-mpls-policy)# cspf-computation-mode ignore-overload-bit
```
The following example displays the configuration output for LSPs and bypass LSPs. They now show the tunnel interface index as part of the output.

```
lsp c2
to 3.3.3.3
tunnel-interface 5001
enable

bypass-lsp byp1
to 3.3.3.3
exclude-interface e3/1
tunnel-interface 5002
enable
```

### History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to display the label withdrawal delay setting.</td>
</tr>
<tr>
<td>5.6.00</td>
<td>This command was modified to display the outbound FEC filter configuration parameter. This command was modified to include <code>use-bypass-liberal</code> under the <code>cspf-computation-mode</code> command output line.</td>
</tr>
<tr>
<td>5.7.00</td>
<td>This command was modified to display the prefix-list configuration instead of the ACL.</td>
</tr>
<tr>
<td>5.8.00</td>
<td>This command was modified to include the line &quot;backup-bw-best-effort&quot; in the <code>show mpls config rsvp</code> command output display.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the next available RSVP LSP tunnel interface index.</td>
</tr>
</tbody>
</table>
**show mpls forwarding**

Displays the MPLS forwarding behavior when the router receives a labeled packet.

**Syntax**

```
show mpls forwarding ip_prefix_addr longer
show mpls forwarding in-label in_label
show mpls forwarding p2p ip_addr
show mpls forwarding p2mp [ dest_prefix detail in_label p2mp_id ]
```

**Parameters**

- `ip_prefix_addr`
  - Displays P2P forwarding entries for the given destination.
- `longer`
  - Displays P2P forwarding entries for the given destination with longer match.
- `in-label`
  - Displays the P2P forwarding entry.
  - `in_label`
    - Specifies the selected in-label.
- `p2p`
  - Displays all P2P forwarding entries for the specified destination or a specified in-label value.
  - `ip_addr`
    - Displays P2P forwarding entries for the given destination.
- `p2mp`
  - Displays all P2MP forwarding entries.
  - `dest_prefix`
    - Specifies the selected destination prefix.
  - `detail`
    - Displays all P2MP forwarding entries in a detailed format.
  - `in_label`
    - Specifies the selected in-label to display.
  - `p2mp_id`
    - Specifies the selected P2MP to display.

**Modes**

User EXEC mode
Usage Guidelines

Command Output

The `show mpls forwarding` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest-prefix</td>
<td>The destination FEC of the LSP.</td>
</tr>
<tr>
<td>In-lbl</td>
<td>The incoming segment or upstream label for the LSP. A value of 0 indicates the absence of the segment.</td>
</tr>
<tr>
<td>Out-lbl</td>
<td>The outgoing segment or downstream label for the LSP.</td>
</tr>
</tbody>
</table>
| Out-intf     | The interface through which the label identified in the 'out-lbl' column has been distributed for the LSP. The 'out-intf' field displays whether an interface/port is an Ethernet port, POS port, or a VE interface. The VE interface ID specified by the vid variable. The out-intf display format for the interface/port is as follows:
  - [e | p] slot/port
    - 'e' represents an Ethernet port.
    - 'p' represents a POS port. |
| Sig          | The signal protocol type associated with the label. Possible values are:
  - L - LDP
  - R - RSVP |
| Next-hop     | The next hop of the LSP. |
| Type         | The 'Type' field identifies a P2MP LSP. |

Examples

The following example displays the output of the `show mpls forwarding` command.

device# show mpls forwarding
Total number of MPLS forwarding entries: 5
<table>
<thead>
<tr>
<th>Dest-prefix</th>
<th>In-lbl</th>
<th>Out-lbl</th>
<th>Out-intf</th>
<th>Sig</th>
<th>Next-hop</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>80.80.80.80/32</td>
<td>1024</td>
<td>1500</td>
<td>e1/12</td>
<td>R</td>
<td>12.12.12.7</td>
<td></td>
</tr>
<tr>
<td>80.80.80.80/32</td>
<td>1025</td>
<td>1502</td>
<td>e1/11</td>
<td>R</td>
<td>11.11.11.7</td>
<td></td>
</tr>
<tr>
<td>80.80.80.80/32</td>
<td>1026</td>
<td>1503</td>
<td>e1/12</td>
<td>R</td>
<td>12.12.12.7</td>
<td></td>
</tr>
<tr>
<td>70.70.70.70/32</td>
<td>1027</td>
<td>3</td>
<td>e1/11</td>
<td>R</td>
<td>11.11.11.7</td>
<td></td>
</tr>
<tr>
<td>70.70.70.70/32</td>
<td>1028</td>
<td>3</td>
<td>e1/12</td>
<td>R</td>
<td>12.12.12.7</td>
<td></td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.1.00</td>
<td>This command was modified to so the 'out-intf' field displays whether an interface/port is either Ethernet or POS.</td>
</tr>
<tr>
<td>5.5.00</td>
<td>This command CLI command syntax changed to <code>show mpls forwarding</code> and includes the options in the parameter section.</td>
</tr>
</tbody>
</table>
show mpls interface

Displays the details about a specific interface.

Syntax

```
show mpls interface [ brief | ethernet slot/port | pos slot/port | tunnel tunnel_id | ve vid ]
```

Parameters

- **brief**: Displays brief interface information.
- **ethernet slot/port**: Specifies the Ethernet port information to display.
- **pos slot/port**: Specifies the POS port information to display.
- **tunnel tunnel_id**: Specifies the Tunnel interface information to display.
- **ve vid**: Specifies the Virtual Ethernet (VE) interface information to display.

Modes

User EXEC mode.

Usage Guidelines

This command operates in all modes.

Command Output

The `show mpls interface ethernet` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface type refers to any one of the following:</td>
</tr>
<tr>
<td>Maximum BW</td>
<td>The maximum outbound bandwidth that can be used on the interface. This TLV reflects the actual physical bandwidth of the interface.</td>
</tr>
</tbody>
</table>
| Maximum reservable BW| The maximum reservable bandwidth on the interface. By default, the maximum reservable bandwidth is the same as the maximum bandwidth for the interface. The user can optionally change the reserved bandwidth on the interface by using the `reservable-bandwidth percentage num` command. The maximum reservable bandwidth displays as either an absolute value or a percentage value of the total interface bandwidth. In the show output displayed above, the maximum reservable bandwidth is configured as a percentage value. However, the percentage value and the absolute value both display in the `show mpls interface ethernet slot/```
Output field | Description
---|---
| port command output so that the user is aware that the bandwidth is configured as a percentage value, not an absolute value.

NOTE
When the maximum reservable bandwidth is configured as an absolute value, the percentage value is not displayed in the output of the `show mpls interface ethernet slot/port` command. Only the absolute value displays in the output.

Admin group | The administrative groups to which this interface belongs, set with the `admin-group` command.
Reservable BW [priority] kbps | The amount of bandwidth not yet reserved on the interface. Eight octets are displayed, indicating the amount of unreserved bandwidth (in kbps) that can be reserved with a hold priority of 0 through 7. The value in each of the octets is less than or equal to the maximum reservable bandwidth.
Last sent reservable BW [priority] kbps | The values in the Unreserved Bandwidth TLV sent in the most recent OSPF-TE LSA. When the device is not sending out OSPF-TE LSAs for the interface, the unreserved bandwidth value for each of the priorities is zero (0).
Configured Protecting bypass LSPs | The name and operational state of any bypass LSPs that are protecting this interface.

Examples

The following example shows the `show mpls interface ethernet` command:

device# show mpls interface ethernet 1/1
el/1
Admin: Up  Oper: Up
Maximum BW: 10000000 kbps, maximum reservable BW: 8000000 kbps (80%)
Admin group: 0x00000000
Reservable BW [priority] kbps:
Last sent reservable BW [priority] kbps:
Configured Protecting bypass lsp: 1
**show mpls label-range**
Displays the MPLS label ranges.

**Syntax**
```
show mpls label-range
```

**Modes**
This command operates under all modes.

**Usage Guidelines**
For an MPLS label, the label range must be between 16 and 499999.

Configuration of in-label values outside of the label range is not permitted.

When the label range is increased or reloaded, there is nothing to be handled. The user gets a wider label range to use.

When the label range is shortened or shifted, and when there are existing static LSPs that have in-labels that fall under the old range—but no longer under the new range—the following guidelines apply:

- They continue to stay UP as the label range change takes effect only after reload.
- When the user reloads with a configuration, that is, with some in-labels now outside of the label range, those LSPs do not come UP if they were or are enabled. However, they remain in the configuration.
- They are allowed to stay in the configuration only so that if the user re-configures the label range to include them and reloads, they can come UP. Also, removing from the configuration due to errors is incorrect behavior.
- The user can disable or enable the LSPs, but they do not come UP.
- The user cannot change the in-labels to another value outside the range, as per point 1 above. If the user changes any in-label successfully to a value inside the range, the user cannot change it back to the old outside-the-range value again. This to follows from point 1.
- When there are LSPs in the configuration that have an in-label value outside the static range, point 3 is the only way the user is able to end up in that state. User configuration of the in-label is not allowed to go outside the range.

**Command Output**
The `show mpls label-range` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS label range</td>
<td>The header for the label ranges configured using commands `label-range [static</td>
</tr>
<tr>
<td>Static</td>
<td>Represents the static label range for transit labels.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>Represents the dynamic label range for transit labels.</td>
</tr>
<tr>
<td>Modified label range</td>
<td>This header displays the values that have been configured, but not yet effective as label range changes require a reload. This section is visible only if a different set of values have been configured to take effect after reload.</td>
</tr>
</tbody>
</table>
Examples

Example of the `show mpls label-range` command display:

device# show mpls label-range
MPLS label range:
  Static           = 16 - 3000
  Dynamic          = 3001 - 499999
Modified label range:*  
  Static           = 16 - 5000
  Dynamic          = 5001 - 499999
*These values will become effective after reload with saved config.
show mpls ldp

Displays the inbound FEC-filter configuration.

Syntax

show mpls ldp

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the inbound FEC-filter configuration.

device# show mpls ldp
Label Distribution Protocol version 1
LSR ID: 10.122.122.122, using Loopback 1 (deleting stops LDP)
Hello interval: Link 5 sec, Targeted 15 sec
Hello time value sent in Hellos: Link 15 sec, Targeted 45 sec
Keepalive interval: 10 sec, Hold time multiple: 3 intervals
Keepalive timeout: 30
Inbound FEC filtering prefix-list list-abc
Tunnel metric: 0
FEC used for auto discovered peers: current 129, configured 129
Label Withdrawal Delay: 30s
Graceful restart: disabled
  Reconnect time: 0 seconds, Max peer reconnect time: 120 seconds
  Recovery time: 0 seconds, Max peer recovery time: 120 seconds
  Forwarding state holding timer: not running
Label Withdrawal Delay: 30s

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to display the label withdrawal delay setting.</td>
</tr>
</tbody>
</table>
show mpls ldp database
Displays the contents of the LSRs LDP Label Information database.

Syntax
show mpls ldp database [ ip_addr ] [ filtered ]

Parameters
ip_addr
Displays the specified peer ID address.

filtered
Displays sessions with filtered mappings.

Modes
User EXEC mode

Usage Guidelines
This database contains all the labels it has learned from each of its LSR peers, as well as all of the labels it has sent to its LDP peers.
This command operates in all modes.

Command Output
The show mpls ldp database command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>The LDP identifiers of this LSR and its peer.</td>
</tr>
<tr>
<td>Downstream label database</td>
<td>Information about labels received from the LDP peer.</td>
</tr>
<tr>
<td>Upstream label database</td>
<td>Information about labels distributed by this LSR to the LDP peer. The device sends the same label for a given prefix to all of its upstream peers.</td>
</tr>
<tr>
<td>Label</td>
<td>The label value received from or distributed to LDP peers. It also displays the label values for VC FECs received from LDP peers or advertised to upstream LDP peers.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The destination route associated with the label. Since the Prefix is not applicable to the VC-FECs, this field indicates that the label is associated with the VC FEC.</td>
</tr>
<tr>
<td>State</td>
<td>Whether the label is actively being used for data forwarding. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>'Installed' indicates that the label is being used with an active LDP-created LSP to forward packets.</td>
</tr>
<tr>
<td></td>
<td>'Retained' indicates that the label is not being used for packet forwarding. Since the LSRs use Liberal Label Retention, these unused labels are retained in the database and not discarded.</td>
</tr>
</tbody>
</table>
Examples

The following example displays the output of the show mpls ldp database command.

device# show mpls ldp database
Session 10.210.210.21:0 - 10.2.2.2:0
Downstream label database:
  Label  Prefix                  State
  1024   10.125.125.25/32(Stale)
  1025   10.220.220.22/32(Stale)

Upstream label database:
  Label  Prefix                  State
  1024   10.125.125.25/32(Stale)

Downstream label database:
  Label  Prefix                  State
  3      10.220.220.22/32        Installed
  1024   10.125.125.25/32        Installed
  983097 VC-FEC                  Retained

Upstream label database:
  Label  Prefix
  983040 VC-FEC
show mpls ldp fec
Displays MPLS forwarding equivalence class (FEC) information.

Syntax

show mpls ldp fec [ summary | vc vc_id
show mpls ldp fec prefix [ ip_addr | ip_addr / subnet-mask-length | filtered [ in | out ] | prefix-filter prefix-list-name ]

Parameters

summary
Displays LDP FEC summary information.

vc vc_id
Displays a detailed view of the FEC VC specified by the vc_id variable.

prefix
Displays Layer 3 prefix FEC information.

ip_addr / subnet-mask-length
Specifies an IP address, with the option of adding subnet mask length.

filtered
Displays only filtered mapping configuration information.

in
Specifies inbound information.

out
Specifies outbound information.

prefix-filter prefix-list-name
Displays the FEC prefixes filtered by the specified prefix-list name.

Modes

Privileged EXEC mode

Usage Guidelines

Command Output

The show mpls ldp fec command options display the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of prefix FECs</td>
<td>The total number of Layer 3 FECs.</td>
</tr>
<tr>
<td>Total number of prefix FECs installed</td>
<td>The total number of Layer 3 FECs installed.</td>
</tr>
<tr>
<td>Total number of prefix FECs filtered(in/out)</td>
<td>The total number of Layer 3 FECs filtered.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total number of prefix FECs with LWD timer running</td>
<td>The total number of Layer 3 FECs with LWD timer running.</td>
</tr>
<tr>
<td>Destination</td>
<td>The IP Prefix associated with the host address or the prefix FEC type.</td>
</tr>
<tr>
<td>State</td>
<td>State of the FEC which indicates the FEC advertised to any LDP session (state equal to 'current'. When it has no session, it is either called 'cur_no_sess' (currently no session) for local FECs or is marked 'retained' for non-local FECs.</td>
</tr>
<tr>
<td>Out-intf</td>
<td>For an ingress FEC, this mentions the output interface to reach to the Next-hop. The 'Out-Intf' field displays the egress interface associated with the FEC entry. When applicable, the 'Out-Intf' field displays a VC interface specified by the vc_id variable.</td>
</tr>
<tr>
<td>Next-hop</td>
<td>For an ingress FEC, this mentions the next-hop IP address.</td>
</tr>
<tr>
<td>Ingress</td>
<td>Whether the FEC is an ingress FEC.</td>
</tr>
<tr>
<td>Egress</td>
<td>Whether the FEC is an egress FEC.</td>
</tr>
<tr>
<td>Filtered</td>
<td>The FEC is filtered Inbound (in) or Outbound (out) or is not filtered (-).</td>
</tr>
<tr>
<td>LWD</td>
<td>Indicate if the Label withdrawal delay timer is active for the FEC.</td>
</tr>
<tr>
<td>LDP FEC summary</td>
<td>Summarized information for LDP FEC.</td>
</tr>
<tr>
<td>Total number of prefix FECs</td>
<td>The total number of prefix FECs in the LDP FEC database.</td>
</tr>
<tr>
<td>Total number of VC-FEC type 128</td>
<td>The total number of VC FECs for type 128. The FEC type for VC FEC can be 128 or 129.</td>
</tr>
<tr>
<td>Total number of VC-FEC type 129</td>
<td>The total number of VC FECs for type 129. The FEC type for VC FEC can be 128 or 129.</td>
</tr>
<tr>
<td>Total number of route update processing errors</td>
<td>The total number of route update processing errors for L3 FEC prefix.</td>
</tr>
<tr>
<td>Total number of L3 VC FEC processing errors</td>
<td>The total number of L3 VC FEC internal processing errors.</td>
</tr>
<tr>
<td>Peer LDP ID</td>
<td>The remote LDP ID of the peer (or local LSR) from where the VC FEC originates.</td>
</tr>
<tr>
<td>VC-ID</td>
<td>The VC identifier associated with the VC FEC.</td>
</tr>
<tr>
<td>VC-Type</td>
<td>The VC Type associated with the VC FEC.</td>
</tr>
<tr>
<td>FEC-Type</td>
<td>The number that identifies the FEC type. The FEC type for VC FEC can be 128 or 129.</td>
</tr>
<tr>
<td>FEC_CB</td>
<td>Memory address of the FEC CB.</td>
</tr>
<tr>
<td>Idx</td>
<td>A monotonically increasing number assigned to each FEC in the LDP FEC tree.</td>
</tr>
<tr>
<td>Pend_notif</td>
<td>Any notification pending on this FEC.</td>
</tr>
<tr>
<td>UM Dist. done</td>
<td>Specifies when Upstream Mapping Distribution is complete.</td>
</tr>
<tr>
<td>Grp_id</td>
<td>Group identifier associated with the VC FEC.</td>
</tr>
<tr>
<td>Local-mtu</td>
<td>The local MTU for a specified VC FEC.</td>
</tr>
<tr>
<td>Remote-mtu</td>
<td>The remote MTU for a specified VC FEC.</td>
</tr>
<tr>
<td>MTU enforcement</td>
<td>The user configured MTU enforcement setting that display 'Enabled' when a specified VC ID is UP.</td>
</tr>
<tr>
<td>Label</td>
<td>MPLS label advertised to the upstream LDP LSR.</td>
</tr>
</tbody>
</table>
Examples

The following example displays the output of the `show mpls ldp fec prefix` command.

device# show mpls ldp fec prefix
Total number of prefix FECs: 4
Total number of prefix FECs installed: 1
Total number of prefix FECs filtered(in/out): 1/0
Total number of prefix FECs with LWD timer running: 0

<table>
<thead>
<tr>
<th>Destination</th>
<th>State</th>
<th>Out-intf</th>
<th>Next-hop</th>
<th>Ingress</th>
<th>Egress</th>
<th>Filtered</th>
<th>LWD</th>
</tr>
</thead>
<tbody>
<tr>
<td>77.77.77.77/32</td>
<td>current</td>
<td>e1/5</td>
<td>5.5.5.6</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>144.144.1.1/32</td>
<td>current</td>
<td>e1/6</td>
<td>6.6.6.6</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>144.144.1.64/32</td>
<td>current</td>
<td>e1/5</td>
<td>5.5.5.6</td>
<td>Yes</td>
<td>No</td>
<td>IN</td>
<td>No</td>
</tr>
<tr>
<td>155.0.0.0/8</td>
<td>current</td>
<td>e1/3</td>
<td>3.3.3.5</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>No</td>
</tr>
</tbody>
</table>

The following example shows the output of the `show mpls ldp fec prefix-filter` command.

device(config)# ip prefix-list listabc deny 172.16.0.0/16 ge 24 le 24
device(config)# ip prefix-list listabc permit 172.16.0.0/16 ge 28 le 28
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# filter-fec list abc in
device(config)# show mpls ldp fec prefix filtered
Total number of prefix FECs: 11

<table>
<thead>
<tr>
<th>Destination</th>
<th>State</th>
<th>Out-intf</th>
<th>Next-hop</th>
<th>Ingress</th>
<th>Egress</th>
<th>Filtered</th>
<th>LWD</th>
</tr>
</thead>
<tbody>
<tr>
<td>77.77.77.77/32</td>
<td>current</td>
<td>e1/5</td>
<td>5.5.5.6</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>144.144.1.1/32</td>
<td>current</td>
<td>e1/6</td>
<td>6.6.6.6</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>No</td>
</tr>
<tr>
<td>144.144.1.64/32</td>
<td>current</td>
<td>e1/5</td>
<td>5.5.5.6</td>
<td>Yes</td>
<td>No</td>
<td>In</td>
<td>No</td>
</tr>
<tr>
<td>155.0.0.0/8</td>
<td>current</td>
<td>e1/3</td>
<td>3.3.3.5</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>No</td>
</tr>
</tbody>
</table>

device(config)#
device(config)# show mpls ldp fec prefix 172.16.8.0/24
FEC_CB: 0x2cd83d78, idx: 4, type: 2, pend_notif: None, fec_definition:22080000
State: current, Ingr: Yes, Egr: No, UM Dist. done: No
Prefix: 172.16.8.0/24
next_hop: 10.55.55.14, out_if: e3/16
Downstream mappings:
Local LDP ID Peer LDP ID Label State CB
10.44.44.44:0 10.14.14.14:0 1024 Retained (f)

The following example shows the output of the `show mpls ldp fec summary` command.

device# show mpls ldp fec summary
LDP FEC summary:
Total number of prefix FECs: 8
Total number of VC-FEC type 128:0
Total number of VC-FEC type 129:0
LDP error statistics:
Total number of route updates processing errors:0
Total number of VC FEC processing errors: 0

The following example shows the output of the `show mpls ldp fec vc` command.

device# show mpls ldp fec vc
Total number of VC FECs:2
Peer LDP ID State VC-ID VC-Type FEC-Type Ingress Egress
10.125.125.1:0 current 100 4 128 Yes Yes
10.125.125.1:0 current 1000 5 128 Yes Yes
The following example shows the output of a MTU mismatch for VC ID of 100, where the VC label received from the remote peer is in a ‘Retained’ state instead of an ‘Installed’ state.

device# show mpls ldp fec vc 100
FEC_CB: 0x293916f8, inx:3, type:128, pend_notif:None
State:current, Ingr:Yes, Egr:Yes, UM Dist. done:Yes
VC_Id:100, vc-type:4, grp_id:0
Local-mtu:2000, remote-mtu:1500, MTU enforcement:enabled

Downstream mappings:
Local LDP ID     Peer LDP Id     Label   State     CB
10.128.128.28:0  10.125.125.1:0  800000  Retained  0x29391328(-1)

Upstream mappings:
Local LDP ID     Peer LDP ID     Label             CB
10.128.128.28:0  10.125.125.1:0  800001            0x29391604(-1)

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>S4.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>S5.00</td>
<td>This command was modified to display label withdrawal delay information.</td>
</tr>
<tr>
<td>S6.00</td>
<td>The filtered options on the <code>show mpls ldp fec filtered</code> command now includes lists for both inbound and outbound FECs.</td>
</tr>
<tr>
<td>S8.00</td>
<td>This command was modified to display the prefix FECs in order of the FEC definition.</td>
</tr>
</tbody>
</table>
show mpls ldp interface
Displays information about the LDP-enabled interfaces on the LSR.

Syntax
show mpls ldp interface [ brief | ethernet slot/port | pos slot/port | tunnel tunnel_id | ve interface_id ]

Parameters
brief
Displays brief interface information.

ethernet slot/port
Displays the specified ethernet port.

pos slot/port
Displays the specified pos interface.

tunnel tunnel_id
Displays the specified tunnel.

ve interface_id
Displays the specified virtual ethernet interface.

Modes
EXEC mode.

Usage Guidelines
Command Output
The show mpls ldp interface command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label-space ID</td>
<td>The label space ID. The second two octets are always zero (0) for LSRs that use per-platform label spaces.</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>The number of LDP peers or adjacencies that have been established on this interface. This number can be greater than one (1) when this is a multi-access network.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The number of seconds between LDP Hello messages.</td>
</tr>
<tr>
<td>Next Hello</td>
<td>The number of seconds before the next LDP Hello message is sent (multicast) to the LDP interface (non-targeted). The LDP Hello message is unicast for a targeted interface. For every neighbor, the next LDP Hello message is sent at a different time. In order to find out when the next LDP Hello message is sent out of any targeted adjacency, use the command show mpls ldp neighbor.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the `show mpls ldp interface` command.

```plaintext
device# show mpls ldp interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Label-space</th>
<th>Nbr</th>
<th>Hello</th>
<th>Next</th>
</tr>
</thead>
<tbody>
<tr>
<td>e4/1</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>0 sec</td>
</tr>
<tr>
<td>(targeted)</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>--</td>
</tr>
<tr>
<td>(targeted)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>--</td>
</tr>
</tbody>
</table>
```
**show mpls ldp neighbor**

Displays information about the connection between this LSP and its LDP-enabled neighbors.

**Syntax**

```
show mpls ldp neighbor [ ip_addr space_id | detail [ ip_addr | space_id ] ]
```

**Parameters**

- `ip_addr`
  - Displays the peer IP address.
- `space_id`
  - The label space identifier.
- `detail`
  - Displays detailed information.
- `ip_addr`
  - The LDP identifier of the neighbor whose details are to be shown.
- `space_id`
  - The label space identifier of the peer. If not provided, global (0) is assumed.

**Modes**

User EXEC mode

**Usage Guidelines**

`show mpls ldp neighbor detail`

This command operates in all modes.

**Command Output**

The `show mpls ldp neighbor detail` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nbr Transport</td>
<td>The transport address of the LDP neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface to which the LDP neighbor is connected. “Targeted” indicates that the session between this device and the neighbor was established using Targeted Hello messages (that is, through extended discovery).</td>
</tr>
<tr>
<td>Nbr LDP ID</td>
<td>The neighbor’s LDP identifier.</td>
</tr>
<tr>
<td>MaxHold</td>
<td>The number of seconds the device waits for its LDP peers to send a Hello message.</td>
</tr>
<tr>
<td>Time Left</td>
<td>The amount of time, in seconds, before the LDP neighbor times out when no Hello message is received from the neighbor.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The Up Time is the time since the LDP adjacency is established. It is displayed in days, hours, minutes, and seconds. When there is no adjacency, then nothing is displayed.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the output of the `show mpls ldp neighbor detail` command.

device# show mpls ldp neighbor detail
Nbr Transport Addr: 10.22.22.1, Interface: e1/1, Nbr LDP ID: 10.22.22.1:0
MaxHold: 44 sec, Time Left: 43 sec, Up Time: 36 min 22 sec
Nbr Transport Addr: 10.22.22.1, Interface: e1/2, Nbr LDP ID: 10.22.22.1:0
MaxHold: 75 sec, Time Left: 74 sec, Up Time: 36 min 27 sec
Nbr Transport Addr: 10.33.33.1, Interface: 31/3, Nbr LDP ID: 10.33.33.1:0
MaxHold: 75 sec, Time Left: 72 sec, Up Time: 36 min 22 sec
Nbr Transport Addr: 10.33.33.1, Interface: targeted, Nbr LDP ID: 10.33.33.1:0
MaxHold: 75 sec, Time Left: 69 sec, Up Time: 35 min 36 sec

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was modified. New variables were introduced under the <code>detail</code> option of the command.</td>
</tr>
</tbody>
</table>
show mpls ldp path

Displays information about active LDP-created LSPs for which the device is an ingress, transit, or egress LSR.

Syntax

```
show mpls ldp path ip_prefix
```

Parameters

- `ip_prefix`
  Designates the IP prefix to display.

Modes

User EXEC mode

Usage Guidelines

The output of this command indicates that the device has received a label for the destination IP prefix (that is, the attached route) from the downstream peer and then advertised a label for that IP prefix to the upstream peer.

This command operates in all modes.

Command Output

The **show mpls ldp path** command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstr-session (label)</td>
<td>The LDP identifier of the upstream peer, as well as the incoming label. Note that upstream session information does not apply to LSPs for which this is the ingress LER. Because the device uses a per-platform label space, the incoming interface for LDP-created LSP is not relevant.</td>
</tr>
<tr>
<td>Downstr-session (label, intf)</td>
<td>The LDP identifier of the downstream peer, as well as the outgoing label and interface. When applicable, the ingress interface <code>intf</code> field displays a VE interface specified by the <code>vid</code> variable. Because the device uses a per-platform label space, the incoming interface for LDP-created LSP is not relevant. Note that downstream session information does not apply to LSPs for which this is the egress LER. When LDP selects its outgoing interface as an RSVP tunnel, the ingress interface <code>intf</code> field displays the RSVP tunnel name.</td>
</tr>
<tr>
<td>Destination route</td>
<td>The destination route bound to this LSP.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the output of the `show mpls ldp path` command.

<table>
<thead>
<tr>
<th>Upstr-session(label)</th>
<th>Downstr-session(label, intf)</th>
<th>Destination route</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.3.3:0(3)</td>
<td>egress</td>
<td>10.1.1.1/32</td>
</tr>
<tr>
<td>10.2.2.2:0(3)</td>
<td>egress</td>
<td>10.1.1.1/32</td>
</tr>
<tr>
<td>10.3.3.3:0(1024)</td>
<td>10.2.2.2:0(3, e2/10)</td>
<td>10.2.2.2/32</td>
</tr>
<tr>
<td>(ingress)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.2.2.2:0(1024)</td>
<td>10.2.2.2:0(3, e2/10)</td>
<td>10.2.2.2/32</td>
</tr>
<tr>
<td>(ingress)</td>
<td>10.3.3.3:0(3, e2/20)</td>
<td>10.3.3.3/32</td>
</tr>
<tr>
<td>(ingress)</td>
<td>10.3.3.3:0(3, e2/20)</td>
<td>10.3.3.3/32</td>
</tr>
</tbody>
</table>
show mpls ldp peer
Displays LDP peering information for each LDP session.

Syntax
show mpls ldp peer [ peer-ip-addr label-id ] brief | detail

Parameters
peer-ip-addr label-id
Displays the peer IP address and the peer label space identifier.
brief
Displays summary LDP peering information.
detail
Displays detailed LDP peering information.

Modes
User EXEC mode

Usage Guidelines
Use this command to view summary or detailed information about LDP sessions and peers. This command operates in all modes.

Command Output
The show mpls ldp peer command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer LDP ID</td>
<td>The LDP identifier of the peer LSR. The first four octets identify the peer LSR IP address; the second two octets identify a label space on the LSR. For LSRs that use per-platform label spaces, the second two octets are always zero (0).</td>
</tr>
<tr>
<td>Local LDP ID</td>
<td>This LSRs LDP identifier.</td>
</tr>
<tr>
<td>State</td>
<td>The LDP session state, as defined in RFC 3036. This can be 'Nonexistent', 'Initialized', 'OpenRec', or 'Operational'.</td>
</tr>
<tr>
<td>Session Status</td>
<td>Whether the session is operationally IP or DOWN.</td>
</tr>
<tr>
<td>Entity Idx</td>
<td>This displays the LDP session entity CB index maintained by the LDP session controller.</td>
</tr>
<tr>
<td>Targeted</td>
<td>Whether the session was established using Targeted Hello messages (that is, through extended discovery).</td>
</tr>
<tr>
<td>Target Adj Added</td>
<td>Whether the targeted adjacency was initiated for this LDP peer.</td>
</tr>
<tr>
<td>Num VLL</td>
<td>Number of VLL instances using the LDP peer.</td>
</tr>
<tr>
<td>Num VPLS</td>
<td>Number of VPLS instances using the LDP peer.</td>
</tr>
<tr>
<td>Rcvd VC FECs</td>
<td>Displays the contents of received VC FECs.</td>
</tr>
<tr>
<td>From</td>
<td>Peer LSR ID where the VC FEC was received from.</td>
</tr>
<tr>
<td>VC ID</td>
<td>The VC identifier associated with the VC FEC.</td>
</tr>
</tbody>
</table>
### Output field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grp_Id</td>
<td>The group identifier associated with the VC FEC.</td>
</tr>
<tr>
<td>VC Type</td>
<td>The VC Type associated with the VC FEC.</td>
</tr>
<tr>
<td>MTU</td>
<td>The MTU value received in a VC Label Matching message from a peer.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays output of the `show mpls ldp peer` command.

```
device# show mpls ldp peer
Peer LDP ID  State       Num- VLL  Num-VPLS-Peer
10.2.2.2:0   Operational  2            0
10.3.3.3:0   Operational  0            0
10.8.8.8:0   Operational  2            0
10.9.9.9:0   Unknown     2            0
10.14.14.14:0 Operational  1            0
```

The following example displays output of the `show mpls ldp peer` with the `detail` keyword.

```
device# show mpls ldp peer detail
Peer LDP ID:10.2.2.2:0, Local LDP ID:10.1.1.1:0, State:Operational
Session Status UP, Entity Idx:4, Targeted:No, Target Adj Added:Yes
Num VLL:2, Num VPLS:0
Rcvd VC-FECs:
  From 10.2.2.2: Label:800001, VC Id:120, Grp_Id:0, VC Type:4, MTU:5000

Peer LDP ID:10.8.8.8:0, Local LDP ID:10.1.1.1:0, State:Operational
Session Status UP, Entity Idx:2, Targeted:Yes, Target Adj Added:Yes
Num VLL:2, Num VPLS:0
Rcvd VC-FECs:
  From 10.8.8.8: Label:16, VC Id:19, Grp_Id:0, VC Type:32773, MTU:5000
  From 10.8.8.8: Label:18, VC Id:18, Grp_Id:0, VC Type:32772, MTU:5555
```
show mpls ldp session
Displays information about LDP sessions between a specified router and VLL peers.

Syntax
```bash
show mpls ldp session [ ip_addr | brief | detail ]
```

Parameters
- `ip_addr`  
  Displays LDP session information for the selected peer IP address.
- `brief`    
  Displays summary LDP session information.
- `detail`   
  Displays detailed LDP session information.

Modes
- Privileged EXEC mode.

Usage Guidelines
Use this command with the `detail` option to display the number of FECs from the peer which are filtered due to the inbound FEC filter configuration.

Command Output
The `show mpls ldp session` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer LDP Ident</td>
<td>The VLL peer’s LDP identifier, consisting of the LSR ID and the label space ID.</td>
</tr>
<tr>
<td>Local LDP Ident</td>
<td>The device’s LDP identifier.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether this LSR is playing an active role in session establishment.</td>
</tr>
<tr>
<td>State</td>
<td>The LDP session state, as defined in RFC 3036. Options are:</td>
</tr>
<tr>
<td></td>
<td>- Nonexistent</td>
</tr>
<tr>
<td></td>
<td>- Initialized</td>
</tr>
<tr>
<td></td>
<td>- OpenRec</td>
</tr>
<tr>
<td></td>
<td>- OpenSent</td>
</tr>
<tr>
<td></td>
<td>- Operational</td>
</tr>
<tr>
<td>Adj</td>
<td>The type of adjacency formed with a peer. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- Link</td>
</tr>
<tr>
<td></td>
<td>- Targeted</td>
</tr>
<tr>
<td>Role</td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>- Active</td>
</tr>
</tbody>
</table>
### Examples

The following example displays the output of the `show mpls ldp peer` command. It displays information about LDP sessions between the device and VLL peers.

```
device# show mpls ldp peer
Peer LDP Ident: 192.168.2.100:1, Local LDP Ident: 10.1.1.1:1
Active: no, State: Operational
TCP connection: 10.1.1.1:646-10.2.2.2:9001, State: ESTABLISHED
Address bound to peer LDP Ident:
  10.1.1.2
  1.1.1.2
  20.1.1.2
  22.2.2.2
```

Display output of the `show mpls ldp session` command showing information about LDP sessions between a specified router and VLL peers.

```
device# show mpls ldp session 10.22.22.22
Peer LDP ID: 10.22.22.22:0, Local LDP ID: 10.24.24.24:0, State: Operational
Adj: Lik, Role: Active, Next keepalive: 0, State: Operational
Keepalive interval: 6 sec, Hold time left: 30 sec
Neighboring interfaces: e1/4
Next-hop addresses received from the peer:
  10.22.22.22 10.40.40.1 10.10.10.2
```

### History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>The command output was modified to display the total number of link and targeted sessions in operational state.</td>
</tr>
<tr>
<td>5.6.00</td>
<td>The command was modified to add the <code>in</code> and <code>out</code> keywords to the filtered option.</td>
</tr>
</tbody>
</table>
**show mpls ldp statistics**

Displays packet statistics for packet types and packet errors.

**Syntax**

```plaintext
show mpls ldp statistic ip_addr
```

**Parameters**

`ip_addr`

Specifies the selected IP address.

**Modes**

EXEC mode.

**Usage Guidelines**

**Command Output**

The `show mpls ldp statistics` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PacketType</td>
<td>The type of LDP packet being counted.</td>
</tr>
<tr>
<td>Total</td>
<td>The number of packets of the type described for the row, sent and received since the Brocade device came UP.</td>
</tr>
<tr>
<td>Since last clear</td>
<td>The number of packets of the type described in the row, sent and received, since issuing the last clear command.</td>
</tr>
<tr>
<td>Errors</td>
<td>The type of packet error being counted. These errors are associated with the received packets only.</td>
</tr>
<tr>
<td>Total</td>
<td>The number of errors of the type described in the row, generated since the Brocade device came UP.</td>
</tr>
<tr>
<td>Since last clear</td>
<td>The number of errors of the type described in the row generated since issuing the last clear command.</td>
</tr>
</tbody>
</table>
Examples

The following example displays the `show mpls ldp statistics` command:

```
device# show mpls ldp statistics

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total</th>
<th>Since last clear</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Received</td>
</tr>
<tr>
<td>Link Hello</td>
<td>215</td>
<td>214</td>
</tr>
<tr>
<td>Targeted Hello</td>
<td>138</td>
<td>110</td>
</tr>
<tr>
<td>Init</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>Notification</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Address</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>AddressWithdraw</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelMapping</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelRequest</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelWithdraw</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelRelease</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelAbortReq</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors</th>
<th>Total</th>
<th>Since last clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcv pkt bad pdu length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt bad msg length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt bad tlv length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt notify unkn tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt notify unkn addr fam</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt incorrect tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt malformed tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt bad traffic parm</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt partial pdu</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt internal error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TCP send error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TCP get send pkt error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TCP memory fail</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Num of TCP socket buffers: 0
```
The following example displays the `show mpls ldp statistics` command for a specific session.

```
device# show mpls ldp statistics 10.10.10.10
Peer IP address: 10.10.10.10
```

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Total Sent</th>
<th>Total Received</th>
<th>Since last clear Sent</th>
<th>Since last clear Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hello Link</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Targeted Hello</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Initialize</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Addr</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>AddrWdrw</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelMap</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>LabelReq</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelWdrw</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelRel</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LabelAbReq</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Errors

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Total</th>
<th>Since last clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcv pkt bad pdu length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt bad msg length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt bad tlv length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt notify unkn tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt notify unkn addr fam</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt missing tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt incorrect tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt malformed tlv</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt bad traffic parm</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt partial pdu</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rcv pkt internal error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TCP send error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TCP get send pkt error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TCP memory fail</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Num of TCP socket buffers</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**show mpls ldp tunnel**

Displays the output sorted by the FEC address, which is the first column of the output.

```
show mpls ldp tunnel ip_addr ip_mask | brief | detail | out-interface [ ethernet slot/port | pos slot/port | ve interface_id ]
```

**ip_addr**

The tunnel destination IP address.

**ip_mask**

The tunnel IP prefix subnet mask.

**brief**

Displays brief information.

**detail**

Displays detailed information.

**out-interface**

Displays LDP tunnels going out of an interface.

**ethernet slot/port**

Displays the specified ethernet port.

**pos slot/port**

Displays the specified port in a POS interface.
Displays the specified POS port.

ve interface_id
Displays the specified Virtual Ethernet (VE) interface.

EXEC mode.

The command displays information about LDP-created LSPs for which this device is the ingress LER.

The command is always sorted by FEC address.

This command operates in all modes.

The following example shows the command output sorted by the FEC address (the 'To' column).

<table>
<thead>
<tr>
<th>To</th>
<th>Oper</th>
<th>Tunnel</th>
<th>Intf</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>UP</td>
<td>tnl0</td>
<td>e1/1</td>
</tr>
<tr>
<td>2.2.2.3</td>
<td>UP</td>
<td>tnl4</td>
<td>e1/1</td>
</tr>
<tr>
<td>3.3.3.3</td>
<td>UP</td>
<td>tnl2</td>
<td>e1/1</td>
</tr>
<tr>
<td>20.1.1.1</td>
<td>UP</td>
<td>tnl1</td>
<td>e1/1</td>
</tr>
</tbody>
</table>

The following example displays the show mpls ldp tunnel command that includes the tunnel-index interface.

```plaintext
device#show mpls ldp tunnel 11.11.11.11
LDP tunnel tnl7, to 11.11.11.11/32
    Tunnel index: 7, metric: 0, status: UP
    Outgoing interface: e1/1, Next-hop index: 0
    Tunnel interface index: 18603
```

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command is modified to include the new parameter <strong>out-interface</strong>.</td>
</tr>
<tr>
<td>5.5.00</td>
<td>The output of this command is modified to include all the paths in the LDP tunnel.</td>
</tr>
<tr>
<td>5.7.00</td>
<td>This command is modified so the output of the <strong>show mpls ldp tunnel</strong> command is always sorted by FEC address.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command is modified to include the tunnel-interface index in the display output.</td>
</tr>
</tbody>
</table>
show mpls lsp
Displays information about configured and active dynamic Multiprotocol Label Switching (MPLS) label-switched paths (LSPs).

Syntax
show mpls lsp autobw-sample | brief | detail | [ down | up [ autobw-sample | detail | extensive | wide ] ] | extensive | name lsp_name autobw-sample | invalid-tunnel-interface wide | wide

Parameters
auto-sample
Displays the sample History for all the auto-bandwidth LSPs.
brief
Displays brief information.
detail
Displays detailed information.
down
Displays operationally DOWN (inactive) LSPs.
up
Displays operationally UP (active) LSPs.
autobw-sample
Displays sample History.
detail
Displays detailed information.
extensive
Displays detailed information with History.
wide
Displays long LSP names.
name lsp_name
Displays information by the specified LSP name.
wide
Displays the long name of the LSP.
invalid-tunnel-interface
Displays LSPs that have an invalid tunnel-interface index because of a bad startup-configuration.
wide
Displays long LSP names.

Modes
EXEC mode.
Usage Guidelines

This command operates in all modes.

The `show mpls lsp brief` command displays the same information as the `show mpls lsp` command.

Command Output

The `show mpls lsp extensive` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the LSP. LSPs display in alphabetical order.</td>
</tr>
<tr>
<td>To</td>
<td>The egress LER for the LSP.</td>
</tr>
<tr>
<td>From</td>
<td>The LSPs source address, configured with the from command. When a source IP address has not been specified for the LSP with the <code>from</code> command, and the LSP has not been enabled, then ‘n/a’ is displayed in the ‘From’ field.</td>
</tr>
<tr>
<td>admin</td>
<td>The administrative state of the LSP. Once the user activates the LSP with the <code>enable</code> command, the administrative state changes from DOWN to UP.</td>
</tr>
<tr>
<td>status</td>
<td>The operational state of the LSP. This field indicates whether the LSP has been established through signaling and is capable of having packets forwarded through it. When the status of the LSP is DOWN, the reason the LSP is down is shown in parentheses ‘( )’. There may be a short after the user enables the LSP that the administrative state of the LSP is UP, but the status is DOWN. Once the LSP establishes through signaling, both the administrative state and the status is UP.</td>
</tr>
<tr>
<td>tunnel interface (primary path)</td>
<td>The MPLS tunnel interface port ID.</td>
</tr>
<tr>
<td>Times primary LSP goes up since enabled</td>
<td>The number of times the status of the LSPs primary path transitions from DOWN to UP.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric for the LSP configured with the <code>metric</code> command.</td>
</tr>
<tr>
<td>Maximum retries</td>
<td>The maximum number of attempts the ingress LER attempts to connect to the egress LER, set with the <code>retry-limit</code> command.</td>
</tr>
<tr>
<td>no. of retries</td>
<td>The number of attempts the ingress LER has made to connect to the egress LER.</td>
</tr>
</tbody>
</table>
| Pri. path    | The name of the primary path for this LSP and whether the path is currently active. up Displays if the primary path is UP. active Displays if the primary path is active. Setup priority Displays if the primary path is active. hold priority The configured hold priority for the LSP. Setup priority The configured setup priority for the LSP. hold priority The configured hold priority for the LSP. Max rate The maximum rate of packets that can go through the LSP (in kbps), set with the `traffic-eng max-rate` command. mean rate The average rate of packets that can go through the LSP (in kbps), set with the `traffic-eng mean-rate` command. max burst The maximum size (in bytes) of the largest burst the LSP can send at the maximum rate, set with the `traffic-eng max-burst` command. Auto-bandwidth template Displays the named auto-bandwidth template configuration information for the path specified by the `show mpls config autobw-template template_name` command. mode Displays when the LSP is in monitor-only mode or monitor-and-signal mode. The default mode is monitor-and-signal. adjustment interval The configured adjustment interval in seconds. Default value: 86400 seconds; range: 300 - 2592000 seconds. adjustment threshold The configured adjustment threshold percentage. Default percentage: 0; range: 0 - 100 percent.
<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minimum bw</td>
<td>The configured minimum bandwidth. Default value: 0 kbps; range: 0 - 2147483647 kbps.</td>
</tr>
<tr>
<td>maximum bw</td>
<td>The configured maximum bandwidth. Default value: 2147483647 kbps; range: 0 - 2147483647 kbps.</td>
</tr>
<tr>
<td>overflow limit</td>
<td>Displays the configured overflow limit.</td>
</tr>
<tr>
<td>underflow limit</td>
<td>The number of samples which have below the threshold to trigger a premature adjustment. Default value: 0; range: 0 - 65535.</td>
</tr>
<tr>
<td>sample-record</td>
<td>The record of all events related to auto-bandwidth of an LSP.</td>
</tr>
<tr>
<td>Constraint-based routing enabled</td>
<td>Whether CSPF is in effect for the LSP.</td>
</tr>
<tr>
<td>Path calculated using constraint-based routing</td>
<td>Whether the explicit path used by the active path was calculated using the constraint-based routing.</td>
</tr>
<tr>
<td>Path calculated using interface constraint</td>
<td>Whether the explicit path used by the active path was calculated using the interface-constraint routing.</td>
</tr>
<tr>
<td>Path cost</td>
<td>The total cost of this path.</td>
</tr>
<tr>
<td>Tie breaking</td>
<td>The tie-breaking method CSPF uses to select a path from a group of equal-cost paths to the egress LER, set with the tie-breaking command.</td>
</tr>
<tr>
<td>hop limit</td>
<td>The maximum number of hops a path calculated by CSPF can have, set with the hop-limit command.</td>
</tr>
<tr>
<td>LDP tunneling enabled</td>
<td>If LDP tunneling is enabled, the line reads ‘yes’. If it is not enabled, the line reads ‘no’.</td>
</tr>
<tr>
<td>Soft preemption enabled</td>
<td>Soft preemption minimizes traffic disruptions and gracefully reroute the preempted LSPs.</td>
</tr>
<tr>
<td>Sec. path</td>
<td>The name of the secondary path for this LSP and whether the path is currently active.</td>
</tr>
<tr>
<td>active</td>
<td>Displays if the secondary path is active.</td>
</tr>
<tr>
<td>Hot-standby</td>
<td>Whether the secondary path is a hot-standby path.</td>
</tr>
<tr>
<td>status</td>
<td>The operational state of the secondary path.</td>
</tr>
<tr>
<td>Setup priority</td>
<td>The name of the secondary path for this LSP and whether the path is currently active.</td>
</tr>
<tr>
<td>hold priority</td>
<td>The configured hold priority for the LSP.</td>
</tr>
<tr>
<td>Max rate</td>
<td>The maximum rate of packets that can go through the LSP (in kbps), set with the traffic-eng max-rate command.</td>
</tr>
<tr>
<td>mean rate</td>
<td>The average rate of packets that can go through the LSP (in kbps), set with the traffic-eng mean-rate command.</td>
</tr>
<tr>
<td>max burst</td>
<td>The maximum size (in bytes) of the largest burst the LSP can send at the maximum rate, set with the traffic-eng max-burst command.</td>
</tr>
<tr>
<td>Auto-bandwidth template</td>
<td>Displays the named auto-bandwidth template configuration information for the path specified by the show mpls config autobw-template template_name command.</td>
</tr>
<tr>
<td>mode</td>
<td>Displays when the LSP is in monitor-only mode or monitor-and-signal mode. The default mode is monitor-and-signal.</td>
</tr>
<tr>
<td>adjustment interval</td>
<td>The configured adjustment interval in seconds. Default value: 86400 seconds; range: 300 - 2592000 seconds.</td>
</tr>
<tr>
<td>adjustment threshold</td>
<td>The configured adjustment threshold percentage. Default percentage: 0; range: 0 - 100 percent.</td>
</tr>
<tr>
<td>minimum bw</td>
<td>The configured minimum bandwidth. Default value: 0 kbps; range: 0 - 2147483647 kbps.</td>
</tr>
<tr>
<td>maximum bw</td>
<td>The configured maximum bandwidth. Default value: 2147483647 kbps; range: 0 - 2147483647 kbps.</td>
</tr>
<tr>
<td>overflow limit</td>
<td>Displays the configured overflow limit value.</td>
</tr>
<tr>
<td>underflow limit</td>
<td>The number of samples which have fallen below the threshold to trigger a premature adjustment. Default value: 0; range: 0 - 65535.</td>
</tr>
<tr>
<td>sample record</td>
<td>The record of all events related to auto-bandwidth of an LSP.</td>
</tr>
<tr>
<td>Constraint-based routing enabled</td>
<td>Whether CSPF is in effect for the LSP.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hop limit</td>
<td>The maximum number of hops a path calculated by CSPF can have, set with the hop-limit command.</td>
</tr>
<tr>
<td>Soft preemption enabled</td>
<td>Soft preemption minimizes traffic disruptions and gracefully reroute the preempted LSPs.</td>
</tr>
<tr>
<td>Active Path attributes:</td>
<td></td>
</tr>
<tr>
<td>Tunnel interface</td>
<td>The MPLS tunnel interface port ID.</td>
</tr>
<tr>
<td>outbound interface</td>
<td>The outbound interface taken by the active path of the LSP. When the egress interface is a VE-enabled interface, the VE interface ID specified by the vid variable.</td>
</tr>
<tr>
<td>Tunnel-interface index</td>
<td>The value of the tunnel-interface index (configured or allocated).</td>
</tr>
<tr>
<td>Tunnel interface</td>
<td>Please note that this specifies the vif index. For example: tnl1 would mean a vif of 1.</td>
</tr>
<tr>
<td>tunnel instance</td>
<td>Source port of the LSP.</td>
</tr>
<tr>
<td>outbound label</td>
<td>The outbound label used by the active path of the LSP.</td>
</tr>
<tr>
<td>Auto-bandwidth running info. mode</td>
<td>Displays when the auto-bandwidth running information mode is in monitor-only mode or monitor-and-signal mode. The default mode is monitor-and-signal.</td>
</tr>
<tr>
<td>adjustment interval</td>
<td>The configured adjustment interval in seconds. Default value: 86400 seconds; range: 300 - 2592000 seconds.</td>
</tr>
<tr>
<td>adjustment threshold</td>
<td>The configured adjustment threshold percentage. Default percentage: 0; range: 0 - 100 percent.</td>
</tr>
<tr>
<td>overflow limit</td>
<td>Displays the configured overflow limit value.</td>
</tr>
<tr>
<td>underflow limit</td>
<td>The number of samples which have to be below the threshold to trigger a premature adjustment.</td>
</tr>
<tr>
<td>minimum bw</td>
<td>The configured minimum bandwidth. Default value: 0 kbps; range: 0 - 2147483647 kbps.</td>
</tr>
<tr>
<td>maximum bw</td>
<td>The configured maximum bandwidth. Default value: 2147483647 kbps; range: 0 - 2147483647 kbps.</td>
</tr>
<tr>
<td>Samples collected</td>
<td>Number of samples collected so far in the current adjustment-interval.</td>
</tr>
<tr>
<td>max sampled bw</td>
<td>The maximum of the samples collected so far in the current adjustment-interval.</td>
</tr>
<tr>
<td>last sample</td>
<td>The last sampled-bandwidth.</td>
</tr>
<tr>
<td>Overflow-count</td>
<td>Displays the number of samples that have consecutively exceeded the adjust-threshold. When a sample does not exceed the threshold, the counter is reset.</td>
</tr>
<tr>
<td>Underflow-count</td>
<td>Displays when the actual traffic rate is much less than the reserved bandwidth.</td>
</tr>
<tr>
<td>Sample-record</td>
<td>Records the sample history.</td>
</tr>
<tr>
<td>Adjustment ignored</td>
<td>This consecutive number of times the adjustment was ignored due to any reason.</td>
</tr>
<tr>
<td>Recorded routes</td>
<td>The addresses recorded by the RECORD_ROUTE object during RSVP signaling.</td>
</tr>
<tr>
<td>Protection codes/Rtr Id flag</td>
<td>The Local out-interface information label and protection flags:</td>
</tr>
<tr>
<td>P: Local</td>
<td></td>
</tr>
<tr>
<td>N: Node</td>
<td></td>
</tr>
<tr>
<td>B: Bandwidth</td>
<td></td>
</tr>
<tr>
<td>I: InUse</td>
<td></td>
</tr>
<tr>
<td>R: RtrID</td>
<td></td>
</tr>
</tbody>
</table>
Examples

The following example shows the output of the `show mpls lsp brief` command:

```
device# show mpls lsp
*: The LSP is taking a Secondary path
    Admin   Oper   Tunnel   Up/Dn   Retry   Active
    Name   To        State   State  Intl     Times  No.     Path
  t1    10.3.3.3  UP      UP*    tnl1     1       5       v2
```

The following example shows the output of the `show mpls lsp detail` command:

```
device(config-mpls)#show mpls lsp detail
LSP c2, to 3.3.3.3, tunnel-interface index: 100
    From: 120.120.120.2, admin: UP, status: DOWN (CSPF fails: code 0)
    Times primary LSP goes up since enabled: 0
    Metric: 0
    Maximum retries: NONE, no. of retries: 0
    Pri. path: NONE, up: no, active: no
    Setup priority: 7, hold priority: 0
    Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
    CSPF-computation-mode configured: use te-metric(global)
    Constraint-based routing enabled: yes
    Path calculated using constraint-based routing: no
    Path calculated using interface constraint: no
    Tie breaking: random, hop limit: 0
    LDP tunneling enabled: no
    Soft preemption enabled: no
    Active Path attributes:
        Tunnel interface: tnl1, outbound interface: e1/6
        Tunnel index: 1, Tunnel instance: 1 outbound label: 3
    Recorded routes:
        Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
        6.6.6.41
```
The following example shows the output of the `show mpls lsp extensive` command:

```plaintext
device# show mpls lsp extensive
LSP lsp1, to 23.23.23.23
  From: 34.34.34.34, admin: UP, status: UP, tunnel interface(primary path): tnl1
  Times primary LSP goes up since enabled: 1
  Metric: 0, Adaptive
  Maximum retries: NONE, no. of retries: 0
  Pri. path: NONE, up: yes, active: yes
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  Auto-bandwidth template: template1, mode: monitor-only
    adjustment interval: 86400 sec, adjustment threshold: 0
    minimum bw: 0 kbps, maximum bw: 2147483647 kbps
    overflow limit: 0, underflow limit: 20, sample-record: disabled
  Constraint-based routing enabled: yes
  Path calculated using constraint-based routing: yes
  Path cost: 20
  Tie breaking: random, hop limit: 0
  LDP tunneling enabled: no
  Soft preemption enabled: no
  Sec. path: via16, active: no
  Hot-standby: no, status: down, adaptive
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  Auto-bandwidth template: NONE, mode: monitor-and-signal
  adjustment interval: 300 sec, adjustment threshold: Table
  minimum bw: 0 kbps, maximum bw: 2147483647 kbps
  overflow limit: 5, underflow limit: 10, sample-record: enabled
  Constraint-based routing enabled: yes
  hop limit: 0
  Soft preemption enabled: no
  Active Path attributes:
    Tunnel interface: tnl1, outbound interface: e4/3
    Tunnel index: 2, Tunnel instance: 1 outbound label: 2049
    Auto-bandwidth running info. Mode: monitor-only
      adjustment interval: 1200 sec(T), adjustment threshold: Table(T)
      overflow limit: 0, underflow limit: 3
      minimum bw: 0 kbps(T), maximum bw: 9647 kbps(T)
    Samples collected: 14, max sampled bw: 0 kbps, last sample: 0 kbps
    Overflow-count: 0, Underflow-count: 2, max-underflow-sample: 34kbps
    Sample-record: enabled(T)
    adjustment due in 1174 seconds
    Adjustment ignored: 0 time(s)
    No adjustment since activation. Current bandwidth: 0 kbps
    Recorded routes:
    Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
    31.31.31.16 -> 161.161.161.1
```

The following example shows the output of the `show mpls lsp wide` command. The full LSP name displays on a single line.

```plaintext
device# show mpls lsp wide
note: LSPs marked with * are taking a Secondary Path

<table>
<thead>
<tr>
<th>Name</th>
<th>To</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Tunnel</th>
<th>Up/Dn</th>
<th>Retry</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunne1</td>
<td>10.3.3.3</td>
<td>UP</td>
<td>UP</td>
<td>tnl0</td>
<td>1</td>
<td>0</td>
<td>--</td>
</tr>
<tr>
<td>tunne12</td>
<td>10.3.3.3</td>
<td>UP</td>
<td>UP</td>
<td>tnl4</td>
<td>1</td>
<td>0</td>
<td>ppath1</td>
</tr>
<tr>
<td>tunneifromsanfranciscotonewyork</td>
<td>10.3.3.3</td>
<td>UP</td>
<td>UP</td>
<td>tnl3</td>
<td>1</td>
<td>0</td>
<td>pathfrom sanfranciscotonewyork</td>
</tr>
</tbody>
</table>
```
The following example shows the bandwidth inherited from the protected LSP.

device# show mpls lsp name to_NY
LSP to NY, to 28.28.28.28
From: 34.34.34.34, admin: UP, status: UP, tunnel interface(primary path): tnl8
Times primary LSP goes up since enabled: 1
Metric: 0
Maximum retries: NONE, no. of retries: 0
Pri. path: to-NY_via_Chicago, up: yes, active: yes
Setup priority: 7, hold priority: 0
Max rate: 0 kbps, mean rate: 2000 kbps, max burst: 0 bytes
CSPF-computation-mode configured: use te-metric(global)
Constraint-based routing enabled: yes
Path calculated using constraint-based routing: yes
Path calculated using interface constraint: no
Path calculated using te-metric
Path cost: 22
Tie breaking: random, hop limit: 0
LDP tunneling enabled: no
Soft preemption enabled: no
Active Path attributes:
Tunnel interface: tnl8, outbound interface: ve11
Explicit path hop count: 3
150.150.150.16 (S) -> 93.93.93.9 (S) -> 28.28.28.28 (L)
Recorded routes:
Protection codes/Rtr Id flag: P: Local N: Node B: Bandwidth I: InUse R: RtrId
150.150.150.16 (PN) -> 93.93.93.9 (P) -> 90.90.90.10
Fast Reroute: facility backup desired, node protection desired
Bandwidth: 2000 kbps (Inherited from Protected LSP)
Backup LSP: UP, out-label: 2048, outbound interface: e1/9 bypass_lsp: to_NY_via_DC
cost: 0
cspf-group computation-mode: disabled
cspf-computation-mode use-bypass-metric: disabled
FRR Forwarding State: Pri(active), Backup(up)

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command is modified to include new events that are logged in the LSP history. The only change is that a new message has been defined for an RRO change. The rest of the fields are unchanged.</td>
</tr>
<tr>
<td>5.5.00</td>
<td>This command is modified to include LSP history with IGP synchronization related history logs when using the extensive option.</td>
</tr>
</tbody>
</table>
| 5.6.00          | This command is modified to show:
|                 | • The **underflow-limit** parameter and the number of consecutive under-flows.  
|                 | • The **adjustment-threshold** is used from the global mode and is indicated by the value of the current rate.  
|                 | • The sample history for the current adjustment interval.  
|                 | • The **autobw-sample** parameter is introduced. |
| 5.8.00          | This command is modified to include "Inherited from Protected LSP" in display output for the **detail**, **extensive**, and **wide** options. |
| 5.9.00          | This command is modified so the output of `show mpls lsp` command in the non-brief versions includes the tunnel-interface index.  
|                 | This command is modified to include an option to display those LSPs that have invalid tunnel-interface index because of bad startup-configuration (invalid-tunnel-interface). |
show mpls lsp_p2mp_xc

Displays hardware information about the forwarding information of hardware that is allocated for the point-to-multipoint (P2MP) cross-connect.

Syntax

    show mpls lsp_p2mp_xc in_label

Parameters

    in_label

    Specifies the MPLS input label value.

Modes

     Privileged EXEC mode.

Usage Guidelines

The show mpls lsp_p2mp_xc command displays information about the forwarding information of hardware that is allocated for the point-to-multipoint (P2MP) cross-connect.

This command operates in all modes.

Examples

The following example displays hardware forwarding statistics on a Brocade NetIron MLX Series device:

device# show mpls lsp_p2mp_xc
P2MP XC TABLE:
TOTAL USED = 2
    IN-LABEL  XC#  FID   MVID  IN-PORT  NUM_OUT_SEGS
  1159      0    0a00a 106   65535     1
  1160      1    0a00b 107   65535     1

device# show mpls lsp_p2mp_xc 1159
TOTAL OUT_SEGs under the given in_label = 1
  BRANCH-ID OUT-LABEL OUT-PORT  NH-ID
     0         0         14          6

Event History -
    Tue Aug 14 02:21:54 2012 P2MP BRANCH ADD
    Tue Aug 14 02:21:54 2012 P2MP XC ADD

flag: 0, pool_index:1, avail_data:270e0800
The following example displays hardware forwarding statistics on a Brocade NetIron CES Series device:

device# show mpls lsp_p2mp_xc
P2MP XC TABLE:
TOTAL USED = 1
IN-LABEL  XC# IP-TTI @ PPCR(1, 2, 3) MPLS-TTI@{PPCR 1, 2, 3} IN-PORT NUM_OUT_SEGS START-DIT
1024      1  65274                  65275                   1/1    2            2049

device# show mpls lsp_p2mp_xc 1024
TOTAL OUT SEGS under the given in_label = 2
BRANCH-ID OUT-LABEL OUT-PORT NH-ID DIT TSI
0        2001    4      0       2049   0
1        2002    4      0       2050   1

Event History -
Tue Aug 14 12:53:17 2012 P2MP BRANCH ADD
Tue Aug 14 12:52:33 2012 P2MP BRANCH ADD
Tue Aug 14 12:52:33 2012 P2MP XC ADD

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
show mpls path

Displays a list of device hops that specifies a route across an MPLS domain.

Syntax

```
show mpls path [path_name | detail | wide]
```

Parameters

- `path_name`
  
  Displays only information for a specified path.

- `wide`
  
  Displays the full path name on a single line.

- `detail`
  
  Displays detailed path information.

Modes

Usage Guidelines

A path is a list of device hops that specifies a route across an MPLS domain. The user can create a path, and then configure LSPs that see the path. When the LSP is enabled, the ingress LER attempts to signal the other LSRs in the path, so that resources can be allocated to the LSP.

This command operates in all modes.

Command Output

The `show mpls path` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path name</td>
<td>The configured name of the path.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of each node in the path. A node corresponds to an MPLS-enabled router in the network.</td>
</tr>
<tr>
<td>Strict or Loose</td>
<td>Whether the node is strict or loose. A strict node means that the router must directly connect to the preceding node. A loose node means that the other routers can reside between the source and destination nodes.</td>
</tr>
<tr>
<td>Usage Count</td>
<td>The number of LSPs that are either currently using or configured to use the path. For example, when an LSP named 'to_sqa' has primary and secondary paths and both paths are configured to use the same MPLS path 'path_to_sqa', then the usage count for 'path_to_sqa' would be two (when no other LSP in the system is configured to use 'path_to_sqa').</td>
</tr>
</tbody>
</table>
Examples

The following example displays the output of the `show mpls path` command.

```
device# show mpls path
Path Name   Address       Strict/loose   Usage Count
              
to110_120 10.110.110.2  Strict         1
          10.120.120.3  Strict

to2_pri   10.10.10.2    Strict         0

to2_sec   10.110.110.2  Strict         0

to3       10.110.110.2  Loose          1
          10.120.120.3  Loose

to3_pri   10.10.10.2    Strict         1
          10.120.120.3  Strict

to3_sec   10.110.110.2  Strict         0
          10.120.120.3  Strict

to4       10.110.110.2  Loose          1
          10.120.120.3  Loose
          10.130.130.4  Loose

to_23     10.110.110.2  Strict         1
          10.20.20.3    Strict
```

The following example displays the `show mpls path wide` command. This option lets the full name of the display on a single line.

```
device# show mpls path wide
Path Name   Address       Strict/loose   Usage Count
            
pathfromsanfranciscotonewyork 10.10.10.2    Strict         1
ppath       10.10.10.2    Strict         1
spath       10.20.20.2    Strict         1
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.00</td>
<td>This command is modified, so the display output displays additional information.</td>
</tr>
<tr>
<td>5.1.00</td>
<td>This command is modified so when using the <code>wide</code> option, the LSP name is displays on a single line. Previously, an LSP name greater than 12 characters was wrapped to multiple lines.</td>
</tr>
</tbody>
</table>
show mpls policy
Displays the current parameter settings configured under the MPLS policy mode.

Syntax
show mpls policy

Modes
MPLS policy configuration mode

Usage Guidelines
The output includes a display of bypass liberal mode if the use bypass liberal keyword was configured as part of the CSPF computation-mode command.

Command Output
The show mpls policy command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current MPLS policy settings:</td>
<td></td>
</tr>
<tr>
<td>CSPF interface constraint</td>
<td>Directs the router to include the interface address as a constraint when it determines the shortest path.</td>
</tr>
<tr>
<td>CSPF-Group computation-mode</td>
<td>Specifies the mode that is used when setting up a fate-sharing group.</td>
</tr>
<tr>
<td>CSPF computation-mode : Use bypass metric</td>
<td>Displays if enabled or disabled. TE metric of TE link for CSPF computation.</td>
</tr>
<tr>
<td>Use bypass liberal</td>
<td>Displays if enabled or disabled. Liberal mode for CSPF facility backup computation.</td>
</tr>
<tr>
<td>Use te-metric</td>
<td>Displays if enabled or disabled. By default, the cspf-computation mode is set to use te-metric.</td>
</tr>
<tr>
<td>Ignore-overload-bit</td>
<td>Displays if enabled or disabled. With this enabled, even when overload bit is set on a transit a router, CSPF at the ingress will not reject any path for new LSPs. If the ignore overload bit is set, already existing transit sessions will not be brought down from ingress on enabling overload bit on transit router.</td>
</tr>
<tr>
<td>TTL propagation for MPLS label</td>
<td>Displays if the TTL propagation for MPLS is enabled or disabled.</td>
</tr>
<tr>
<td>IPVPN</td>
<td>Displays if IPVPN is enabled or disabled.</td>
</tr>
<tr>
<td>IP over MPLS</td>
<td>Displays if IP over MPLS is enabled or disabled.</td>
</tr>
<tr>
<td>Inter-AS-route filtering</td>
<td>When the user enables inter-AS-route filtering, the RTM does not send any inter-AS routes to MPLS.</td>
</tr>
<tr>
<td>Intra-AS iBGP route filtering</td>
<td>Displays if intra-AS iBGP route filtering is enabled or disabled.</td>
</tr>
<tr>
<td>Ingress tunnel accounting</td>
<td>Displays if ingress tunnel accounting is enabled or disabled.</td>
</tr>
<tr>
<td>Polling interval for MPLS LSP traffic statistics</td>
<td>Displays the polling interval, in seconds.</td>
</tr>
<tr>
<td>Advertise TE parameters via</td>
<td>Displays which level option enables LSPs with TE extensions. The level-1 option enables TE extensions for the IS-IS level-1 domain. The level-2 option enables LSPs with TE extensions for the IS-IS level-2 domains.</td>
</tr>
<tr>
<td>Handle IGP neighbor down event - ISIS</td>
<td>Displays if IS-IS is handling the IGP neighbor DOWN event.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Handle IGP neighbor down event - OSPF</td>
<td>Displays if OSPF is handling the IGP neighbor DOWN event.</td>
</tr>
<tr>
<td>LSP rapid retry</td>
<td>Displays if LSP rapid retry is enabled or disabled.</td>
</tr>
<tr>
<td>Maximum number of retries</td>
<td>Displays the maximum number of times the port will try the health check.</td>
</tr>
<tr>
<td></td>
<td>Values are from 3 - 64. The default value is 7.</td>
</tr>
<tr>
<td>LSP periodic retry time</td>
<td>Displays the LSP periodic retry time in seconds.</td>
</tr>
<tr>
<td>FRR backup/detour retry time</td>
<td>Displays the FRR backup and detour retry time in seconds.</td>
</tr>
<tr>
<td>Auto-bandwidth</td>
<td>Displays if auto-bandwidth is enabled or disabled.</td>
</tr>
<tr>
<td>Sample-interval</td>
<td>On changing the sample-interval the sample-timer is reset for all the</td>
</tr>
<tr>
<td></td>
<td>auto-bandwidth LSPs. Any rate information already collected so far in the</td>
</tr>
<tr>
<td></td>
<td>current sample-interval is considered a valid sample.</td>
</tr>
<tr>
<td>Maximum samples recorded per LSP</td>
<td>Displays the maximum samples recorded per LSP.</td>
</tr>
<tr>
<td>Soft preemption cleanup-timer</td>
<td>Interval time between when the path is taken down and the new LSP is</td>
</tr>
<tr>
<td></td>
<td>established. Any traffic attempting to use the LSP is lost.</td>
</tr>
<tr>
<td>MPLS TE Periodic Flooding Timer</td>
<td>Displays the timer in seconds. All MPLS interfaces are checked every</td>
</tr>
<tr>
<td></td>
<td>three minutes by default. TE advertisements are triggered when there is a</td>
</tr>
<tr>
<td></td>
<td>difference in the available bandwidth and advertised available bandwidth.</td>
</tr>
<tr>
<td>MPLS TE flooding thresholds:</td>
<td>Displays global UP thresholds. UP values are 10, 20, 30, 40, 50, 55, 60,</td>
</tr>
<tr>
<td></td>
<td>65, 70, 85, 90, 92, 93, 94, 95, 96, 97, 98, 99, 100.</td>
</tr>
<tr>
<td></td>
<td>Displays global DOWN thresholds. DOWN values are 99, 98, 97, 96, 95, 94,</td>
</tr>
<tr>
<td></td>
<td>93, 92, 91, 90, 85, 80, 75, 70, 65, 60, 55, 50, 45, 30, 20, 10.</td>
</tr>
<tr>
<td>Global UP thresholds</td>
<td>Displays default UP thresholds. UP values are 10, 20, 30, 40, 50, 55, 60,</td>
</tr>
<tr>
<td></td>
<td>65, 70, 75, 80, 85, 90, 92, 93, 94, 95, 96, 97, 98, 99, 100.</td>
</tr>
<tr>
<td>Default UP thresholds</td>
<td>Displays default DOWN thresholds. DOWN values are 99, 98, 97, 96, 95, 94,</td>
</tr>
<tr>
<td></td>
<td>93, 92, 91, 90, 85, 80, 75, 70, 65, 60, 55, 50, 40, 30, 20, 10.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the output of the `show mpls policy` command:

```
device# show mpls policy
Current MPLS policy settings:
  CSPF interface constraint: disabled
  CSPF-Group computation-mode: disabled
  Use bypass metric: disabled
  Use bypass liberal: disabled
  Use te-metric (default), Ignore-overload-bit: disabled
  TTL propagation for MPLS label: disabled, IPVPN: disabled, IP over MPLS: enabled
  Inter-AS route filtering: enabled, Intra-AS iBGP route filtering: disabled
  Ingress tunnel accounting: disabled
  Polling interval for MPLS LSP traffic statistics: 300 seconds
  Advertise TE parameters via: OSPF
  Handle IGP neighbor down event - ISIS: No OSPF: No
  LSP rapid retry: enabled, maximum number of retries: no limit
  LSP periodic retry time: 30 seconds
  FRR backup/detour retry time: 30 seconds
  Auto-bandwidth: enabled, sample-interval: 60 seconds
  Maximum samples recorded per LSP: 1500
  MPLS TE Periodic Flooding Timer: 180 seconds
  MPLS TE flooding thresholds:
    Global UP thresholds: None
    Global DOWN thresholds: None
    Default UP thresholds: 15 30 45 60 75 80 85 90 95 96 97 98 99 100
    Default DOWN thresholds: 99 98 97 96 95 90 85 80 75 60 45 30 15
```
## History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was modified to include bypass liberal output when the <code>use bypass liberal</code> keyword is configured in the <code>cspf-computation-mode</code> command.</td>
</tr>
<tr>
<td>5.8.00</td>
<td>This command was modified to include 'CSPF computation-mode' information in the display output.</td>
</tr>
</tbody>
</table>
**show mpls route**
Displays the contents of the MPLS routing table.

**Syntax**
```
show mpls route [ ip_addr [ / ip_mask ] ]
```

**Parameters**
- `ip_addr`
  Specifies the destination IP address.
- `/ ip-mask`
  Specifies the IP subnet mask.

**Modes**
User EXEC mode

**Usage Guidelines**
With LDP ECMP LER tunnels, the output for one tunnel could be greater than one line where each line shows one outgoing path - the repetitive lines do not have the ‘Destination’ and ‘Tnnl’ columns filled because they match what is in the first line.

**Command Output**
The `show mpls route` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination for the route. This can be either the address of the egress LER in an LSP, or a configured alias.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The address of the egress LER in the LSP. When the destination address is not a network alias, the gateway is the same as the destination address.</td>
</tr>
<tr>
<td>Tnnl</td>
<td>The address of the egress LER in the LSP. When the destination address is not a network alias, the gateway is the same as the destination address.</td>
</tr>
<tr>
<td>Port</td>
<td>The MPLS tunnel interface associated with the LSP. The port field displays whether an interface/port is an Ethernet port, POS port, or a VE interface. The VE interface ID is specified by the <code>vid</code> variable. When applicable, the egress interface of the routing entry displays the VE interface. The port display format for interface or port is as follows:</td>
</tr>
</tbody>
</table>
  - `[e|p] slot or port` |
  - ‘e’ represents an Ethernet port |
  - ‘p’ represents a POS port |
| Label        | The MPLS label received from the downstream router. |
| Sig          | The signal protocol type associated with the label. Possible values are: |
  - `L` – LDP |
  - `R` – RSVP |
### Examples

The following example displays the `show mpls route` command.

```
device# show mpls route
Total number of MPLS tunnel routes: 4
R:RSVP L:LDP S:Static O:Others

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Tnnl</th>
<th>Port</th>
<th>Label</th>
<th>Sig</th>
<th>Cost</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 10.12.12.12/32</td>
<td>10.12.12.12</td>
<td>tnl1</td>
<td>e2/1</td>
<td>3</td>
<td>R</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 10.12.12.12/32</td>
<td>10.12.12.12</td>
<td>tnl15</td>
<td>e2/1</td>
<td>3</td>
<td>L</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 10.13.13.13/32</td>
<td>10.13.13.13</td>
<td>tnl4</td>
<td>e1/1</td>
<td>3</td>
<td>L</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4 10.77.77.12/32</td>
<td>10.12.12.12</td>
<td>tnl10</td>
<td>e2/1</td>
<td>3</td>
<td>L</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

### History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>With LDP ECMP LER tunnels, the output for one tunnel could be greater than one line where each line shows one outgoing path.</td>
</tr>
</tbody>
</table>
show mpls rsvp interface
Displays the status of RSVP on devices where it is enabled.

Syntax

```plaintext
show mpls rsvp interface brief | detail | [ ethernet | pos | ve slot/port ]
```

Parameters

- **brief**: Displays brief interface information.
- **detail**: Displays detailed interface information.
- **ethernet slot/port**: Displays the specified ethernet port.
- **pos slot/port**: Displays the specified POS port.
- **ve slot/port**: Displays the specified virtual ethernet interface.

Modes

Privileged EXEC mode.

Usage Guidelines

clear mpls rsvp statistics

This command operates in all modes.

Command Output

The `show mpls rsvp interface` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Whether the interface is UP or DOWN.</td>
</tr>
<tr>
<td>MD5</td>
<td>Whether RSVP message authentication is enabled on the interface.</td>
</tr>
<tr>
<td>RelMsg</td>
<td>Whether RSVP reliable messaging is enabled on the interface.</td>
</tr>
<tr>
<td>Bundle</td>
<td>Whether RSVP bundle messages are enabled on the interface.</td>
</tr>
<tr>
<td>SRefresh</td>
<td>Whether RSVP summary refresh is enabled on the interface.</td>
</tr>
<tr>
<td>Num of OutSegAct/Inact/Resv</td>
<td>Out segments are traffic connections on the link. These connections may be active or inactive. 'Resv' represents the number of active out segments with a nonzero mean rate.</td>
</tr>
<tr>
<td>Num of Preempts</td>
<td>Number of times lower-priority LSPs have been preempted on this interface.</td>
</tr>
</tbody>
</table>
Examples

The following example displays the `show mpls rsvp interface` command:

```
device# show mpls rsvp interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>MD5</th>
<th>RelMsg</th>
<th>Bundle</th>
<th>SRefresh</th>
<th>Act/Inact/Resv</th>
<th>Preempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>e3/2 (Trunk8)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>0/0/0</td>
<td>0</td>
</tr>
<tr>
<td>e3/4 (Trunk9)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>0/0/0</td>
<td>0</td>
</tr>
<tr>
<td>e3/6</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>0/0/0</td>
<td>0</td>
</tr>
<tr>
<td>e3/7 (Trunk2)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>1699/0/1684</td>
<td>1142</td>
</tr>
<tr>
<td>e3/8 (Trunk6)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>167/0/106</td>
<td>0</td>
</tr>
<tr>
<td>e4/3 (Trunk3)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>2526/0/2526</td>
<td>1471</td>
</tr>
<tr>
<td>e4/5 (Trunk4)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>8421/0/8421</td>
<td>774</td>
</tr>
<tr>
<td>e7/1 (Trunk17)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>8480/0/8421</td>
<td>5479</td>
</tr>
<tr>
<td>e7/2 (Trunk19)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>7489/0/7484</td>
<td>0</td>
</tr>
<tr>
<td>e9/3 (Trunk7)</td>
<td>Up</td>
<td>OFF</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>178/0/158</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following example displays a shorter output, using the `show mpls rsvp interface brief` command:

```
device# show mpls rsvp interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>MD5 Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>e2/1</td>
<td>Up</td>
<td>OFF</td>
</tr>
<tr>
<td>e2/2</td>
<td>Dn</td>
<td>OFF</td>
</tr>
<tr>
<td>e4/1</td>
<td>Dn</td>
<td>OFF</td>
</tr>
<tr>
<td>e4/2</td>
<td>Dn</td>
<td>OFF</td>
</tr>
</tbody>
</table>
```

(output truncated)
show mpls rsvp neighbor

Displays RSVP neighbors that were discovered dynamically during the exchange of RSVP packets.

Syntax

show mpls rsvp neighbor [ ipv4address | detail ]

Parameters

ipv4address
  Specifies the IP address of a learned neighbor.

detail
  Displays RSVP neighbor information in a detailed format.

Modes

Privileged EXEC mode.

Usage Guidelines

Use this command to display all the current RSVP neighbors for this router.

The ‘RR’ and ‘MsgID’ flags in this command show the ability of the neighbor to support Refresh Reduction and Message IDs respectively.

The ‘MsgID’ field is set to ‘YES’ in the following cases:

- This field is defaulted to ‘YES’ initially.
- It is set to ‘YES’ if the neighbor sends a message containing a Message ID.
- It is also set to ‘YES’ if the remote MPLS interface is configured to send Message IDs to this neighbor.

The ‘MsgID’ field is set to ‘NO’ when the peer rejects a message (with a ‘PathErr’ or ‘ResvErr’) because it contains a Message ID object.

If the neighbor sends a NACK to a Message ID object that is sent and then subsequently sends a Path or Resv message that does not contain a Message ID, then RSVP sets this field to ‘NO’. This allows RSVP to inter-operate with devices that do not support Message IDs.

This command operates in all modes.

Command Output

The show mpls rsvp neighbor command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSVP neighbors learnt</td>
<td>Number of neighbors the router has learned.</td>
</tr>
<tr>
<td>Nbr Address</td>
<td>Address of the learned neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface where the neighbor has been detected.</td>
</tr>
</tbody>
</table>
**Output field** | **Description**
--- | ---
**State** | Current status of the neighbor.  
**UP** - Router can detect RSVP-TE Hello messages from the neighbor.  
**DOWN** - Router has received a failure from the neighbor or change in the sequence numbers in RSVP Hello messages sent by the neighbor.

**Last_Change** | Time elapsed since the neighbor state changed.  
Format: days: hours: minutes: seconds.

**Number of LSPs to or from this Nbr** | This field displays the number of LSPs or RSVP sessions using this next-hop (neighbor).(Detail mode only.)

**Hello-interval** | **Hello-interval** - Frequency at which RSVP-TE Hello Request messages are sent on the interface, in seconds.

**Hello-tolerance** | **Hello-tolerance** - The number of hello periods that may pass without receiving a complete Hello message before the Hello session times out. (Detail mode only.)

**Hello Tx/Rx Count** | Number of Hello packets sent to or received from the neighbor.

**RR/MsgID Support** | Indicates if Refresh Reduction and Message ID support is enabled and or supported by the neighbor.  
(Y - Enabled, N - Disabled)

**No Hello message received since** | This field displays how far back (in seconds) the last RSVP Hello (Request OR Ack) message was received.

**Time left to send next Hello Req** | This field is valid and displays the time only when the Neighbor supports RSVP Hellos. Otherwise, it displays `'-'`. (Detail mode only.)

**Remote instance** | Identifier provided by the remote router during Hello messages (Dest_Instance or Neighbor_Src_Instance). (Detail mode only.)

**Local instance** | Identifier sends to the neighbor during Hello messages (Src_Instance). (Detail mode only.)

**Refresh Reduction** | Indicates if Refresh Reduction is enabled or supported by the neighbor. (Detail mode only.)

**Message ID** | Indicates if Message ID support is enabled by the neighbor. (Detail mode only.)

---

**Examples**

The following example displays the output of the `show mpls rsvp neighbor` command.

```plaintext
device# show mpls rsvp neighbor
RSVP neighbors learnt: 4
Nbr Address Interface State Last_Change HelloTx/Rx RR/MsgID
10.152.152.15 e1/2 UP 10:2:31:44 8498/8349 Y/Y
10.92.98.9 e1/12 UP 0:6:39:36 3995/3587 N/Y
10.31.31.15 e4/3 DOWN 6:6:39:36 3000/1267 N/Y
10.92.99.9 e3/2 UP 0:0:31:44 2995/0 N/N

device# show mpls rsvp neighbor 10.92.98.9
Nbr Address: 92.92.98.9, Interface: e1/12, State: UP
Last changed time (d:h:m:s): 0:6:39:38, Number of active LSPs to or from this Nbr: 22
Hello sent: 3995, received: 3587, Hello-interval: 15 sec, Hello-tolerance: 5
No Hello message received since: 5 sec
Time left to send next Hello Req: 10 sec
Remote instance: 0x65c6b2, Local instance: 0x5a4f9f21
Refresh Reduction: Disabled, Message ID: Enabled

device# show mpls rsvp neighbor 10.1.1.1
RSVP neighbor with the provided IP address does not exist
```
## History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
show mpls rsvp session

Displays information regarding Resource reSerVation Protocol (RSVP) sessions.

Syntax

show mpls rsvp session [ backup | brief | bypass | destination | detail | detour | down | egress | extensive | in-interface | ingress | name sess-name | out-interface | p2mp | p2p | ppend | transit | up | wide ]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

bypass
Displays bypass session.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name sess-name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

Displays sessions in soft preemption pending state.

Displays a transit session.

Displays up session.

Displays long LSP names.

**Modes**

User EXEC mode

**Usage Guidelines**

The `show mpls rsvp session brief` command displays the same information as the `show mpls rsvp session` command. This command operates in any mode.

**Command Output**

The `show mpls rsvp session` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress RSVP</td>
<td>Displays information about ingress RSVP sessions.</td>
<td>show mpls rsvp session&lt;br&gt;show mpls rsvp session detail&lt;br&gt;show mpls rsvp session extensive</td>
</tr>
<tr>
<td>Transit RSVP</td>
<td>Displays information about transit RSVP sessions.</td>
<td>show mpls rsvp session&lt;br&gt;show mpls rsvp session detail&lt;br&gt;show mpls rsvp session extensive</td>
</tr>
<tr>
<td>Egress RSVP</td>
<td>Displays information about egress RSVP sessions.</td>
<td>show mpls rsvp session&lt;br&gt;show mpls rsvp session detail&lt;br&gt;show mpls rsvp session extensive</td>
</tr>
<tr>
<td>To</td>
<td>Destination (egress LER) of the session.</td>
<td>show mpls rsvp session&lt;br&gt;show mpls rsvp session detail&lt;br&gt;show mpls rsvp session extensive&lt;br&gt;show mpls rsvp session wide</td>
</tr>
<tr>
<td>From</td>
<td>Source (ingress LER) of the session; the source address for the LSP configured with the <code>from</code> command.</td>
<td>show mpls rsvp session&lt;br&gt;show mpls rsvp session detail&lt;br&gt;show mpls rsvp session extensive&lt;br&gt;show mpls rsvp session wide</td>
</tr>
<tr>
<td>St</td>
<td>State can be UP or DOWN.</td>
<td>show mpls rsvp session&lt;br&gt;show mpls rsvp session detail&lt;br&gt;show mpls rsvp session extensive</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
<td>Command</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Style</strong></td>
<td>The RSVP reservation style. Possible values are <em>Fixed Filter (FF)</em>, <em>Wildcard Filter (WF)</em>, or <em>Shared Explicit (SE)</em>.</td>
<td>show mpls rsvp session wide</td>
</tr>
<tr>
<td><strong>Lbl_In</strong></td>
<td>The label for inbound packets on this LSP.</td>
<td>show mpls rsvp session wide</td>
</tr>
<tr>
<td><strong>Lbl_Out</strong></td>
<td>The label applied to outbound packets on this LSP.</td>
<td>show mpls rsvp session wide</td>
</tr>
<tr>
<td><strong>Out_if</strong></td>
<td>The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the <code>vid</code> variable.</td>
<td>show mpls rsvp session wide</td>
</tr>
<tr>
<td><strong>LSPname</strong></td>
<td>The name of the LSP.</td>
<td>show mpls rsvp session wide</td>
</tr>
<tr>
<td><strong>Time left in seconds</strong></td>
<td>The amount of time left for the PATH or RESV refreshes.</td>
<td>show mpls rsvp session detail</td>
</tr>
<tr>
<td><strong>Tspec</strong></td>
<td>Traffic engineering specification for the LSP, including the max-rate (&quot;peak&quot;), mean rate (&quot;rate&quot;), number of burst bytes (&quot;size&quot;), maximum policed unit (&quot;M&quot;—or maximum packet size), and minimum policed unit (&quot;m&quot;—or minimum packet size).</td>
<td>show mpls rsvp session detail</td>
</tr>
<tr>
<td><strong>Explicit path hop count</strong></td>
<td>The number of explicit hops used in this RSVP session.</td>
<td>show mpls rsvp session extensive</td>
</tr>
<tr>
<td><strong>Received RRO count</strong></td>
<td>The number of Record Route Objects received on this RSVP session.</td>
<td>show mpls rsvp session extensive</td>
</tr>
<tr>
<td><strong>PATH sentto</strong></td>
<td>Address of the next LSR in the LSP, and the interface used to reach this LSR. When applicable, ‘PATH sentto’ displays a VE interface specified by the <code>vid</code> variable.</td>
<td>show mpls rsvp session extensive</td>
</tr>
<tr>
<td><strong>PATH rcvfrom</strong></td>
<td>Address of the previous LSR in the LSP, and the interface used to reach this LSR. When the session is downstream only, then it is displayed. When applicable, ‘PATH rcvfrom’ displays a VE interface specified by the <code>vid</code> variable.</td>
<td>show mpls rsvp session extensive</td>
</tr>
</tbody>
</table>
| **PATH history** | Displays history of the last 20 RSVP event. Each event contains:  
  - Event index (used to provide the number of events).  
  - Time stamp  
  - File name and line number where the event is logged. | show mpls rsvp session extensive |
Examples

The following example displays the `show mpls rsvp session` command.

```
device(config)# show mpls rsvp session
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
      DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
      RP:Repaired Session BYI: Bypass Ingress

Ingress RSVP: 10 session(s)
To          From             St Style Lbl_In Lbl_Out Out_If LSPname
10.22.22.22 10.11.11.11      Up FF    -      3       e4/3   xmr2
10.33.33.33 10.11.11.11(DI)  Up SE    -      3       e4/4   rj-vpls
10.33.33.33 10.11.11.11      Up SE    -      1039   e1/15  rj-vpls

Transit RSVP: 1009 session(s)
To          From             St Style Lbl_In Lbl_Out Out_If LSPname
10.22.22.22 10.33.33.33      Up SE    1024   3       e4/3   2
10.22.22.22 10.33.33.33(DI)  Up SE    1072   1319   e2/4   toxmr2frr-

Egress RSVP: 62 session(s)
To          From             St Style Lbl_In Lbl_Out Out_If LSPname
10.11.11.11 10.22.22.22(DE)  Up SE     3     -       -      toxm1-frr
10.11.11.11 10.22.22.22    Up SE     3     -       -      toxm1-frr
10.11.11.11 10.44.44.44    Up SE     3     -       -      toxm1-frr
10.11.11.11 10.22.22.22(DI)  Up SE     3     -       -      toxm1-frr

The following command allows the user to display the full LSP name in a single line.

device# show mpls rsvp session wide

Ingress RSVP: 4 session(s)
10.3.3.3 10.2.2.2       Up SE     3     e1/1    tunnel1
10.3.3.3 10.10.10.10(BI) Dn  -     -     e1/3    tunnel1
10.3.3.3 10.2.2.2(BYI)   Up SE     3     e1/3    by1
10.3.3.3 10.2.2.2       Up SE     3     e1/1    tunnelfromsanfranciscotonewyork
10.3.3.3 10.10.10.10(BI) Dn  -     -     e1/3    tunnelfromsanfranciscotonewyork
10.3.3.3 10.2.2.2(BYI)   Up SE     3     e1/3    bypasstunnelfromsfotonewyork

Transit RSVP: 0 session(s)
Egress RSVP: 0 session(s)
```

the following example displays the command using the wide parameter.

```
device# show mpls rsvp session backup wide

Ingress RSVP: 2 session(s)
To          From             St Style Lbl_In Lbl_Out Out_If LSPname
10.3.3.3 10.2.2.2       Up SE     3     e1/1    tunnel1
10.3.3.3 10.10.10.10(BI) Dn  -     -     e1/3    tunnel1
10.3.3.3 10.2.2.2(BYI)   Up SE     3     e1/1    by1
10.3.3.3 10.2.2.2       Up SE     3     e1/1    tunnelfromsanfranciscotonewyork
10.3.3.3 10.10.10.10(BI) Dn  -     -     e1/3    tunnelfromsanfranciscotonewyork
10.3.3.3 10.10.10.10(BI) Dn  -     -     e1/3    tunnelfromsanfranciscotonewyork

Egress RSVP: 0 session(s)
Transit RSVP: 0 session(s)
```
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6.00</td>
<td>This command is enhanced to include a new option that allows the display of RSVP events such as state transitions and events associated with RSVP sessions.</td>
</tr>
<tr>
<td>5.1.00</td>
<td>This command is enhanced to display the full LSP name on a single line. Previously, a long LSP name (greater than 12 characters) was text wrapped in multiple lines. Enhanced command: <code>show mpls rsvp session wide</code>.&lt;br&gt;The show mpls rsvp session command is enhanced to display if the session is downstream only. Command: <code>show mpls rsvp session detail</code>.</td>
</tr>
<tr>
<td>5.5.00</td>
<td>This command is enhanced to include the following new filters:&lt;br&gt;• `p2mp</td>
</tr>
<tr>
<td>5.8.00</td>
<td>This command is modified to display explicitly on the protected session if it has bandwidth protection or not. It will display only on the protected session. Available on the <code>show mpls rsvp session detail</code> command.</td>
</tr>
</tbody>
</table>
show mpls rsvp session backup
Displays the Reserved Reservation Protocol (RSVP) facility backup session.

Syntax
show mpls rsvp session backup [ active [ brief | destination | detail | egress | extensive | in-interface | ingress | name | out-interface | p2mp | p2p | ppend | protection-available | protection-unavailable | transit | up | wide ]

Parameters
active
Displays active backup and or detour sessions.
brief
Displays brief session information.
destination
Displays the destination IP address
detail
Displays detailed session information.
egress
Displays the egress session.
extensive
Displays extensive session information.
in-interface
Displays RSVP session coming into an interface.
ingress
Displays the ingress session.
name
Displays session by name.
out-interface
Displays RSVP sessions going out on an interface.
p2mp
Displays point to multipoint sessions.
p2p
Displays point to point sessions.
ppend
Displays sessions in a soft preemption pending state.
protection-available
Displays sessions with protection available.
protection-unavailable
**Show Commands**

Displays sessions with protection unavailable.

**transit**
Displays transit session.

**up**
Displays UP session.

**wide**
Displays long LSP names.

### Modes

User EXEC mode

### Usage Guidelines

### Examples

The following example displays the output from the command using the wide option.

```
device#show mpls rsvp session backup wide
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
      DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
      RP:Repaired Session BYI: Bypass Ingress
Ingress RSVP: 2 session(s)
To      From             St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.3.3.3 10.2.2.2         Up  SE     -       3        e1/1    tunnel1
10.3.3.3 10.10.10.10(BI)  Dn  -      -       -        e1/3    tunnel1
10.3.3.3 10.2.2.2         Up  SE     -       3        e1/1    tunnelfromsanfranciscotonewyork
10.3.3.3 10.10.10.10(BI)  Dn  -      -       -        e1/3    tunnelfromsanfranciscotonewyork
Transit RSVP: 0 session(s)
Egress RSVP: 0 session(s)
```
show mpls rsvp session brief
Displays the Reserved Reservation Protocol (RSVP) brief session information.

Syntax
show mpls rsvp session brief [ backup | bypass | destination | detour | down | egress | in-interface | ingress name | out-interface | p2mp | p2p | ppend | transit | up ]

Parameters
backup
Displays facility backup session.
bypass
Displays bypass session.
destination
Displays the destination IP address.
detour
Displays detour session.
down
Displays inactive session.
egress
Displays egress session.
in-interface
Displays RSVP sessions going out on an interface.
ingress
Displays the ingress session.
name
Displays session by name.
out-interface
Displays RSVP session going up.
p2mp
Displays point to multipoint.
p2p
Displays point to point.
ppend
Displays sessions in soft preemption pending status.
transit
Displays transit session.
up
Displays UP session.

**Modes**
User EXEC mode

**Usage Guidelines**
This command operates in all modes.

The `show mpls rsvp session brief` command displays the same information as the `show mpls rsvp session` command.

**Command Output**
The `show mpls rsvp session brief` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress RSVP</td>
<td>Information about ingress RSVP sessions.</td>
</tr>
<tr>
<td>Transit RSVP</td>
<td>Information about transit RSVP sessions.</td>
</tr>
<tr>
<td>Egress RSVP</td>
<td>Information about egress RSVP sessions.</td>
</tr>
<tr>
<td>To</td>
<td>Destination (egress LER) of the session.</td>
</tr>
<tr>
<td>From</td>
<td>Source (ingress LER) of the session; the source address for the LSP that was configured with the from command.</td>
</tr>
<tr>
<td>St</td>
<td>State can be UP or DOWN.</td>
</tr>
<tr>
<td>Style</td>
<td>The RSVP reservation style. Possible values are FF (Fixed Filter), WF (Wildcard Filter), or SE (Shared Explicit).</td>
</tr>
<tr>
<td>Lbl_In</td>
<td>The label for inbound packets on this LSP.</td>
</tr>
<tr>
<td>Lbl_Out</td>
<td>The label applied to outbound packets on this LSP.</td>
</tr>
<tr>
<td>Out_If</td>
<td>The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the vid variable.</td>
</tr>
<tr>
<td>LSPName</td>
<td>The name of the LSP.</td>
</tr>
</tbody>
</table>
Examples

The following example shows the `show mpls rsvp session` command.

```
device(config)#show mpls rsvp session
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
      DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
      RP:Repaired Session BYI: Bypass Ingress

Ingress RSVP: 10 session(s)

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>St</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out_If</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.22.22.22</td>
<td>10.11.11.11</td>
<td>Up</td>
<td>FF</td>
<td>3</td>
<td>e4/3</td>
<td>xmr2</td>
<td></td>
</tr>
<tr>
<td>10.33.33.33</td>
<td>10.11.11.11(DI)</td>
<td>Up</td>
<td>SE</td>
<td>3</td>
<td>e4/4</td>
<td>rj-vpls</td>
<td></td>
</tr>
</tbody>
</table>

Transit RSVP: 1009 session(s)

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>St</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out_If</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.22.22.22</td>
<td>10.33.33.33</td>
<td>Up</td>
<td>SE</td>
<td>1024</td>
<td>3</td>
<td>e4/3</td>
<td>2</td>
</tr>
<tr>
<td>10.22.22.22</td>
<td>10.33.33.33(DI)</td>
<td>Up</td>
<td>SE</td>
<td>1072</td>
<td>1319</td>
<td>e2/4</td>
<td>toxmr2frr-</td>
</tr>
</tbody>
</table>

Egress RSVP: 62 session(s)

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>St</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out_If</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.11.11.11</td>
<td>10.22.22.22(DE)</td>
<td>Up</td>
<td>SE</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>toxmr1</td>
</tr>
<tr>
<td>10.11.11.11</td>
<td>210.22.22.22(DE)</td>
<td>Up</td>
<td>SE</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>toxmr1</td>
</tr>
<tr>
<td>10.11.11.11</td>
<td>10.22.22.22</td>
<td>Up</td>
<td>SE</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>toxmr1</td>
</tr>
<tr>
<td>10.11.11.11</td>
<td>10.44.44.44</td>
<td>Up</td>
<td>FF</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>toxmr1</td>
</tr>
</tbody>
</table>
```
**show mpls rsvp session bypass**

Displays *Reserved Reservation Protocol (RSVP)* bypass sessions.

**Syntax**

```plaintext
show mpls rsvp session bypass [ brief | destination | detail | down | extensive | in-interface | ingress | name | out-interface | p2mp | p2p | ppend | up | wide ]
```

**Parameters**

- **brief**
  Displays brief session information.
- **destination**
  Destination IP address.
- **detail**
  Displays detailed session information.
- **down**
  Displays inactive section.
- **extensive**
  Displays extensive session information.
- **in-interface**
  Displays RSVP sessions coming into an interface.
- **ingress**
  Displays ingress session.
- **name**
  Displays session by name.
- **out-interface**
  Displays RSVP sessions going out on an interface.
- **p2mp**
  Displays point to multipoint sessions.
- **p2p**
  Displays point to point sessions.
- **ppend**
  Displays sessions in soft preemption pending status.
- **up**
  Displays Up session.
- **wide**
  Displays lonf LSP names.
Modes

EXEC mode.

Usage Guidelines

Examples

The following example displays the output of the command with the detail parameter.

device# show mpls rsvp session bypass detail
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
DE:Egress Detour BI:Ingress Backup BM:Merged Backup BE:Egress Backup
RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 2

Ingress RSVP: 2 session(s)
To From St Style Lbl_In Lbl_Out Out_IIf LSPname
1.1.4.1 1.1.1.1(BYI) Up SE - 1024 ve33
GREEN_DOWN_PE1toP1_VE1111-11.11.1.1-29
Tunnel ID: 48, LSP ID: 1
Time left in seconds (PATH refresh: 24, ttd: 4235431
RESV refresh: 18, ttd: 113)
Tspec: peak 19200 kbps rate 19200 kbps size 0 bytes m 20 M 65535
Setup Priority: 7 Holding Priority: 0
Session attribute flags:0x04
(SE Style)
Explicit path hop count: 3
11.1.3.0 (S) -> 23.1.100.1 (S) -> 32.1.10.1 (S)
Received RRO count: 3
Protection codes/Rtr Id flag: P: Local N: Node B: Bandwidth I: InUse R: RtrId
11.1.3.0 -> 23.1.100.1 -> 32.1.10.1
PATH sentto: 11.1.3.0 (ve33 ) (MD5 OFF), Message ID: --
RESV rcvfrom: 11.1.3.0 (ve33 ) (MD5 OFF), Message ID: --
show mpls rsvp session destination
Displays the selected Resource Reservation Protocol (RSVP) session destination IP address.

Syntax

    show mpls rsvp [ destination dest_ip ] [ in-interface | out-interface | backup | brief | bypass | detail | detour | egress | ingress | extensive | name session_name | ppend | transit | up | down | wide | p2mp | p2p ]

Parameters

destination dest_ip
Displays the selected destination IP address.

in-interface
Displays RSVP sessions coming into an interface.

out-interface
Displays RSVP session going out on an interface.

backup
Displays facility backup session.

brief
Display brief session information.

bypass
Displays bypass session.

detail
Displays detailed session information.

detour
Displays detour session.

egress
Displays egress session.

ingress
Displays ingress session.

extensive
Displays extensive session information.

name session_name
Displays session by specified name.

ppend
Displays sessions in soft preemption pending state.

transit
Displays transit session.

up
Show Commands

Displays UP session.

down
Displays inactive session.

wide
Displays long LSP names.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

Modes
User EXEC mode

Usage Guidelines

Examples
The following example displays the output of the command.

device(config)#show mpls rsvp session dest 10.30.30.30 source 10.10.10.10 tun 1
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 1
To   From     St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
10.30.30.30  10.10.10.10  Up  FF     1024    3        e3/1    t1
show mpls rsvp session detail
Displays detailed Reserved Reservation Protocol (RSVP) session information.

Syntax
show mpls rsvp session detail [ backup | bypass | destination | detour | down | egress | in-interface | ingress | name | out-interface | p2mp | p2p | ppend | transit | up ]

Parameters
backup
Displays facility backup session.
bypass
Displays bypass session.
destination
Destination IP address.
detour
Displays detour session.
down
Displays inactive session.
egress
Displays egress session.
in-interface
Displays RSVP sessions coming into an interface.
ingress
Displays ingress session.
name
Displays session by name.
out-interface
Displays RSVP sessions going out on an interface
p2mp
Displays point to multipoint sessions.
p2p
Displays point to point sessions.
ppend
Displays sessions in a soft preemption pending state.
transit
Displays transit session.
up
Displays UP session.

**Modes**

**EXEC mode.**

**Usage Guidelines**

**Examples**

The following example displays the output of the command when the session is only downstream.

```
device# show mpls rsvp session detail
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
      DE:Egress Detour  BI:Ingress Backup  BM:Merged Backup  BE:Egress Backup
      RP:Repaired Session  BYI: Bypass Ingress

Total Number of such sessions are: 1

To              From                 St Style Lbl_In  Lbl_Out Out_If LSPname
28.28.28.28     34.34.34.34          Up SE    2050    2049    e1/8   to_NY
Tunnel ID: 4, LSP ID: 1
Time left in seconds (PATH refresh: 44, ttd: 119
RESV refresh: 7, ttd: 152)
Tspec: peak 300 kbps rate 300 kbps size 0 bytes m 20 M 65535
Setup Priority: 7 Holding Priority: 0
Session attribute flags:0x1f
   (Label recording,SE Style,Protection: Local,Bandwidth,Node)
Fast Bypass: Facility backup desired
Setup priority: 7, hold priority: 0
Bandwidth: 300 kbps, hop limit: 255
Backup LSP: UP. Nexthop (node) protection available.
Bandwidth protection available.
Up/Down times: 1, num retries: 0
cost: 0
  Path cspf-group computation-mode: disabled
  Path cspf-computation-mode use-bypass-metric: disabled,
Explicit path hop count: 2
  93.93.93.9 (S) -> 90.90.90.10 (S)
  Received RRO count: 2
Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
  93.93.93.9 (P) -> 90.90.90.10
PATH rcvfrom: 150.150.150.15 (ve11) (MD5 OFF), Message ID: --
PATH sentto: 93.93.93.9 (e1/8) (MD5 OFF), Message ID: --
RESV rcvfrom: 93.93.93.9 (e1/8) (MD5 OFF), Message ID: --

To              From                 St Style Lbl_In  Lbl_Out Out_If LSPname
28.28.28.28     35.35.35.35(BI)      Up -     2050    3       e1/10  to_NY
Tunnel ID: 4, LSP ID: 1
Time left in seconds (PATH refresh: 0, ttd: 4280803)
Tspec: peak 300 kbps rate 300 kbps size 0 bytes m 20 M 65535
Setup Priority: 7 Holding Priority: 0
Session attribute flags:0x06
   (Label recording,SE Style)
Explicit path hop count: 1
  28.28.28.28 (S)
PATH rcvfrom: None (downstream only)
PATH sentto: 28.28.28.28 (e1/10) (MD5 OFF), Message ID: --
Riding bypass lsp: DUT_16-93.93.93.16-28.28.28.28-2
```

Show Commands
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.00</td>
<td>This command is modified to display when the session is only downstream.</td>
</tr>
</tbody>
</table>
show mpls rsvp session detour
Displays the Reserved Reservation Protocol (RSVP) detour session.

Syntax
show mpls rsvp session { detour [ active | brief | destination | detail | down | egress | extensive | in-interface | inactive | ingress | name | out-interface | p2mp | p2p | ppend | protection-available | protection-unavailable | transit | up wide }

Parameters
active
Displays active backup and detour sessions.
brief
Displays brief session information.
destination
Destination IP address.
detail
Displays detailed session information.
down
Displays inactive session.
egress
Displays egress session.
extensive
Displays extensive session information.
in-interface
Displays RSVP sessions coming into an interface.
inactive
Displays inactive, but UP, backup or detour session.
ingress
Displays ingress session.
name
Displays session by name.
out-interface
Displays RSVP sessions going out on an interface.
p2mp
Displays point to multipoint sessions.
p2p
Displays point to point sessions.
ppend
Displays sessions in a soft preemption pending state.

**protection-available**
Displays sessions with protection available.

**protection-unavailable**
Displays sessions with protection unavailable.

**transit**
Displays transit session.

**up**
Displays UP session.

**wide**
Displays long LSP names.

**Modes**
User EXEC mode

**Usage Guidelines**

**Examples**
The following example displays a typical output of the command.

```
device# show mpls rsvp session detour
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI_Ingress Backup  BM:Merged Backup  BE:Egress Backup
       RP:Repaired Session  EVI:Bypass Ingress
Total Number of such sessions are: 0
Ingress RSVP: 0 session(s)
Transit RSVP: 0 session(s)
Egress RSVP: 0 session(s)
```
show mpls rsvp session down
Displays inactive Reserved Reservation Protocol (RSVP) sessions.

Syntax
show mpls rsvp session down [ backup | brief | bypass | destination | detail | detour | egress | extensive | in-interface | ingress | name | out-interface | p2mp | p2p | ppend | transit | wide ]

Parameters
backup
Displays facility backup session.
brief
Displays brief session information.
bypass
Displays bypass session.
destination
Destination IP address.
detail
Displays detailed session information.
detour
Displays detour session.
egress
Displays egress session.
extensive
Displays extensive session information.
in-interface
Displays RSVP sessions coming into an interface.
ingress
Displays ingress session.
name
Displays session by name.
out-interface
Displays RSVP sessions going out on an interface.
p2mp
Displays point to multipoint session.
p2p
Displays point to point session.
ppend
Displays sessions in a soft preemption pending state.

**transit**
Displays transit session.

**wide**
Displays long LSP names.

## Modes
User EXEC mode

## Usage Guidelines

## Examples

The following example displays the output of the command using the wide option.

```
device#show mpls rsvp session down wide
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
      DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
      RP:Repaired Session BI: Bypass Ingress
Total Number of such sessions are: 59
Transit RSVP:  59 session(s)
To    From                  St Style Lbl_In  Lbl_Out Out_If LSPname
10.0.11.11  10.0.0.5          Dn -    -    -    e1/2    to_AR11_autoBW_11
10.0.11.12  10.0.0.5          Dn -    -    -    e1/2    to_AR11_autoBW_12
10.0.11.13  10.0.0.5          Dn -    -    -    e1/2    to_AR11_autoBW_13
10.0.11.14  10.0.0.5          Dn -    -    -    e1/2    to_AR11_autoBW_14
```
**show mpls rsvp session extensive**

Displays extensive Reserved Reservation Protocol (RSVP) session information.

**Syntax**

```
show mpls rsvp session extensive [ backup | bypass | destination | detour | down | egress | in-interface | ingress | name | out-interface | p2mp | p2p | ppend | transit | up ]
```

**Parameters**

- **backup**
  - Displays facility backup session.

- **bypass**
  - Displays bypass session.

- **destination**
  - Destination IP address.

- **detour**
  - Displays detour session.

- **down**
  - Displays inactive session.

- **egress**
  - Displays egress session.

- **in-interface**
  - Displays RSVP sessions coming into an interface.

- **ingress**
  - Displays ingress sessions.

- **name**
  - Displays session by name.

- **out-interface**
  - Displays RSVP sessions going out of an interface.

- **p2mp**
  - Displays point to multipoint sessions.

- **p2p**
  - Displays point to point sessions.

- **ppend**
  - Displays sessions in a soft preemption pending state.

- **transit**
  - Displays transit session.

- **up**
  -
Displays UP sessions.

Modes
User EXEC mode

Usage Guidelines

Command Output

The `show mpls rsvp session extensive` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress RSVP</td>
<td>Displays information about ingress RSVP sessions.</td>
</tr>
<tr>
<td>Transit RSVP</td>
<td>Displays information about transit RSVP sessions.</td>
</tr>
<tr>
<td>Egress RSVP</td>
<td>Displays information about egress RSVP sessions.</td>
</tr>
<tr>
<td>From</td>
<td>Source (ingress LER) of the session; the source address for the LSP that was configured with the <code>from</code> command.</td>
</tr>
<tr>
<td>State (St)</td>
<td>State can be UP or DOWN.</td>
</tr>
<tr>
<td>Style</td>
<td>The RSVP reservation style. Possible values are Fixed Filter (FF), Wildcard Filter (WF), or Shared Explicit (SE).</td>
</tr>
<tr>
<td>Lbl_In</td>
<td>The label for inbound packets on this LSP.</td>
</tr>
<tr>
<td>Lbl_Out</td>
<td>The label applied to outbound packets on this LSP.</td>
</tr>
<tr>
<td>Out_IF</td>
<td>The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the <code>vid</code> variable.</td>
</tr>
<tr>
<td>LSPName</td>
<td>The name of the LSP.</td>
</tr>
<tr>
<td>Time left in seconds</td>
<td>The amount of time left for the PATH or RESV refreshes.</td>
</tr>
<tr>
<td>Tspec</td>
<td>Traffic engineering specification for the LSP, including the max-rate (&quot;peak&quot;), mean rate (&quot;rate&quot;), number of burst bytes (&quot;size&quot;), maximum policed unit (&quot;M&quot;-or maximum packet size), and minimum policed unit (&quot;m&quot;-or minimum packet size).</td>
</tr>
<tr>
<td>Explicit path hop count</td>
<td>The number of explicit hops used in this RSVP session.</td>
</tr>
<tr>
<td>Received RRO count</td>
<td>The number of Record Route Objects received on this RSVP session.</td>
</tr>
<tr>
<td>PATH sentto</td>
<td>Address of the next LSR in the LSP, and the interface used to reach this LSR. When applicable, <code>PATH sentto</code> displays a VE interface specified by the <code>vid</code> variable.</td>
</tr>
<tr>
<td>PATH rcvfrom</td>
<td>Address of the previous LSR in the LSP, and the interface used to reach this LSR. When the session is downstream only, then it is displayed. When applicable, <code>PATH rcvfrom</code> displays a VE interface specified by the <code>vid</code> variable.</td>
</tr>
<tr>
<td>PATH history</td>
<td>Displays history of the last 20 RSVP event. Each event contains:</td>
</tr>
<tr>
<td></td>
<td>• Event index (used to provide the number of events).</td>
</tr>
<tr>
<td></td>
<td>• Time stamp</td>
</tr>
<tr>
<td></td>
<td>• File name and line number where the event is logged.</td>
</tr>
<tr>
<td></td>
<td>• Event description and extra information associated with each event.</td>
</tr>
</tbody>
</table>
Examples

The following example displays the command output containing the contents of the History buffer for the last 20 RSVP events.

device# show mpls rsvp session extensive
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BY: Bypass Ingress

Ingress RSVP: 7 session(s)
To          From            St Style Lbl_In Lbl_Out Out_If LSPname
10.33.33.33 10.11.11.11(DI) Up SE -      3       e4/4   rj-vpls
Tunnel ID: 1, LSP ID: 1
Time left in seconds (PATH refresh: 10, ttd: 4288020
       RESV refresh: 0, ttd: 4288177)
Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
Explicit path hop count: 1
10.0.0.6 (S)
Received RRO count: 1
Protection codes/Rtr Id flag: P: Local N: Node B: Bandwidth I: InUse R: RtrId
10.0.0.6
Detour Sent: Number of PLR and Avoid Node ID pair(s): 1
   [1]: PLR: 10.1.1.1 Avoid Node: 10.1.1.2
PATH sentto: 10.0.0.6 (e4/4) (MD5 OFF)
RESV rcvfrom: 10.0.0.6 (e4/4) (MD5 OFF)
PATH history:
1 Dec 10 11:57:59 Query route to 10.33.33.33: nhop 10.0.0.6
2 Dec 10 11:57:59 Tx PATH: out if(e4/4), flg(0x01000500/0x0000000a)
3 Dec 10 11:57:59 Rx RESV: label(3), flg(0x01100500/0x0000000a)
4 Dec 10 11:57:59 Tx cnnt req: hdl(0x0010c001), flg(0x01100500/0x0000000a)
5 Dec 10 11:57:59 Start TC event(NEW_FLOW): action(0x0000000a)
6 Dec 10 11:57:59 Rx cnnt resp: hdl(0x0010c001), flg(0x01100500/0x0000000a)
7 Dec 10 11:57:59 Complete TC event(NEW_FLOW)
RESV history:
1 Dec 10 11:57:59 Add RSB: style(SE), filterSpec(1), flg(0x00000000)
2 Dec 10 11:57:59 Add filterSpec: 10.11.11.1, label(3)

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6.00</td>
<td>This command was enhanced to include a new option that allows the display of RSVP events such as state transitions and events associated with RSVP sessions.</td>
</tr>
</tbody>
</table>
show mpls rsvp session (ingress/egress)
Displays Reserved Reservation Protocol (RSVP) ingress or egress session.

Syntax
show mpls rsvp session ingress [ backup | brief | bypass | destination | detail | detour | down | extensive | in-interface | name | out-interface | p2mp | p2p | ppend | up | wide ]
show mpls rsvp session egress [ backup | brief | destination | detail | detour | down | extensive | in-interface | name | out-interface | p2mp | p2p | ppend | up | wide ]

Parameters
backup
Displays facility backup session.

brief
Displays brief session information.

bypass
(For ingress only) Displays bypass session information.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Displays detour session.

down
Displays inactive session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Show Commands

Displays sessions in a soft preemption pending status.

**up**
Displays UP session.

**wide**
Displays long LSP names.

**Modes**
User EXEC mode

**Usage Guidelines**
show mpls rsvp session (interface)

Displays RSVP sessions that are coming into (in-interface) or going out to (out-interface) an interface.

Syntax

- show mpls rsvp session in-interface { ethernet slot / port | pos slot / port | ve interface_id }
- show mpls rsvp session out-interface { ethernet slot / port | pos slot / port | ve interface_id }

Parameters

- ethernet slot / port
  Displays the specified Ethernet port.
- pos slot / port
  Displays the specified POS port.
- ve interface_id
  Displays the specified Virtual Ethernet Interface ID.

Modes

User EXEC mode

Usage Guidelines
show mpls rsvp session name
Displays the Reserved Reservation Protocol (RSVP) session by name.

Syntax

```show mpls rsvp session name session_name [ backup | brief | bypass | destination | detail | detour | down | egress | extensive | in-interface | ingress | out-interface | p2mp | p2p | ppend | transit | up | wide | extensive ]```

Parameters

- **backup**
  Displays facility backup session information.

- **brief**
  Displays brief session information.

- **bypass**
  Display bypass session information.

- **destination**
  Destination IP address information.

- **detail**
  Displays detailed session information.

- **detour**
  Displays detour session information.

- **down**
  Displays inactive session information.

- **egress**
  Displays egress session information.

- **extensive**
  Displays extensive session information.

- **in-interface**
  Displays RSVP sessions coming into an interface.

- **ingress**
  Displays ingress session information.

- **out-interface**
  Displays RSVP sessions going out on an interface.

- **p2mp**
  Displays point to multipoint session information.

- **p2p**
  Displays point to point session information.

- **ppend**
  Displays extended session information.
Displays sessions in the soft preemption pending state.

**transit**
Displays transit session information.

**up**
Displays up session information.

**wide**
Displays the long LSP name.

### Modes

User EXEC mode

### Usage Guidelines

### Command Output

The `show mpls rsvp session name` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td>Destination (egress LER) of the session.</td>
</tr>
<tr>
<td>From</td>
<td>Source (ingress LER) of the session; the source address for the LSP that was configured with the <strong>from</strong> command.</td>
</tr>
<tr>
<td>St</td>
<td>State can be UP or DOWN.</td>
</tr>
<tr>
<td>Style</td>
<td>The RSVP reservation style. Possible values are FF (Fixed Filter), WF (Wildcard Filter), or SE (Shared Explicit).</td>
</tr>
<tr>
<td>Lbl_in</td>
<td>The label for inbound packets on this LSP.</td>
</tr>
<tr>
<td>Lbl_out</td>
<td>The label applied to outbound packets on this LSP.</td>
</tr>
<tr>
<td>Out_if</td>
<td>The outbound interface displays the egress interface for a session. When applicable, the outbound interface displays a VE interface specified by the <strong>vid</strong> variable.</td>
</tr>
<tr>
<td>LSPname</td>
<td>The name of the LSP.</td>
</tr>
<tr>
<td>Tunnel ID</td>
<td>A numerical value that identifies the tunnel being configured.</td>
</tr>
<tr>
<td>Time left in seconds</td>
<td>The amount of time left for the PATH or RESV refreshes.</td>
</tr>
<tr>
<td>Tspec</td>
<td>Traffic engineering specification for the LSP, including the max-rate (&quot;peak&quot;), mean rate (&quot;rate&quot;), number of burst bytes (&quot;size&quot;), maximum policed unit (&quot;M&quot;—or maximum packet size), and minimum policed unit (&quot;m&quot;—or minimum packet size).</td>
</tr>
<tr>
<td>Setup Priority</td>
<td>An LSPs setup priority is considered during admission control, and its hold priority is considered when bandwidth is allocated to the LSP.</td>
</tr>
<tr>
<td></td>
<td>The setup priorities are expressed as numbers between zero (0) (highest priority level) and seven (7) (lowest priority level).</td>
</tr>
<tr>
<td>Holding Priority</td>
<td>The hold priority is considered when bandwidth is allocated to the LSP.</td>
</tr>
<tr>
<td></td>
<td>The hold priorities are expressed as numbers between zero (0) (highest priority level) and seven (7) (lowest priority level).</td>
</tr>
<tr>
<td>Received RRO count</td>
<td>The number of Record Route Objects received on this RSVP session.</td>
</tr>
<tr>
<td>PATH sentto</td>
<td>Address of the next LSR in the LSP, and the interface used to reach this LSR. When applicable, PATH sentto displays a VE interface specified by the <strong>vid</strong> variable.</td>
</tr>
<tr>
<td>PATH history</td>
<td>Displays history of the last 20 RSVP events. Each event contains:</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|              | • Event index (used to provide the number of events).  
|              | • Time stamp.  
|              | • File name and line number where the event is logged.  
|              | • Event description and extra information associated with each event. |

| RESV history | Displays reservation history. |
| Session history | Displays session history. |

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>The number of Path messages sent and received. Path messages store information about the state of the path along the LSRs in the LSP.</td>
</tr>
<tr>
<td>Resv</td>
<td>The number of RESV messages sent and received. RESV messages include FF (Fixed Filter), WF (Wildcard Filter), and SE (Shared Explicit) messages.</td>
</tr>
<tr>
<td>PathErr</td>
<td>The number of PathErr messages sent and received.</td>
</tr>
<tr>
<td>RevErr</td>
<td>The number of ResvErr messages sent and received.</td>
</tr>
<tr>
<td>PathTear</td>
<td>The number of PathTear messages sent and received. PathTear messages cause path states to be deleted.</td>
</tr>
<tr>
<td>ResvTear</td>
<td>The number of ResvTear messages sent and received. ResvTear messages cause reservation states to be deleted.</td>
</tr>
<tr>
<td>ResvConf</td>
<td>The number of reservation confirmation messages sent and received.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PATH state timeout</td>
<td>The PATH timeout.</td>
</tr>
<tr>
<td>RESV state timeout</td>
<td>The reservation confirmation timeout.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rcv pkt proc error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>The number of Path messages received with a packet processing error.</td>
</tr>
<tr>
<td>Resv</td>
<td>The number of RESV messages received with a packet processing error.</td>
</tr>
<tr>
<td>PathErr</td>
<td>The number of PathErr messages received with a packet processing error.</td>
</tr>
<tr>
<td>RevErr</td>
<td>The number of ResvErr messages received with a packet processing error.</td>
</tr>
<tr>
<td>PathTear</td>
<td>The number of PathTear messages received with a packet processing error.</td>
</tr>
<tr>
<td>ResvTear</td>
<td>The number of reservation confirmation messages received with a packet processing error.</td>
</tr>
<tr>
<td>ResvConf</td>
<td>The number of reservation confirmation messages received with a packet processing error.</td>
</tr>
</tbody>
</table>
Examples

The following example shows how the protocol statistics display when using the extensive option.

device# show mpls rsvp session name lsp1 extensive
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
       DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BY: Bypass Ingress

Total Number of such sessions are: 1
To              From                 St  Style  Lbl_In  Lbl_Out  Out_If  LSPname
Tunnel ID: 1, LSP ID: 1
Time left in seconds (PATH refresh: 26, ttd: 3889074
       RESV refresh: 4, ttd: 141)
Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
Setup Priority: 7  Holding Priority: 0
Session attribute flags:0x00
Received RRO count: 1
Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
22.22.22.14
PATH sentto: 22.22.22.14 (e2/1 ) (MD5 OFF), Message ID: 1
RESV rcvfrom: 22.22.22.14 (e2/1 ) (MD5 OFF), Message ID: --
PATH history:
<SNIP>
17 Dec 11 20:40:23 Tx Resv to TE-MIB: flg(0x00005404/0x00000000)
RESV history:
1 Dec 11 20:40:23 Add RSB: style(FF), filterSpec(1), flg(0x00000000)
2 Dec 11 20:40:23 Add filterSpec: 12.12.12.12/1, label(3)
Session history:
1 Dec 11 20:40:23 A new PSB 0x30ee03c8 created. stack[1]=0x00000001 stack[2]=0x21bab8d4
<SNIP>
12 Dec 11 20:40:23 TC-action LDB_CONNECT completed

Protocol Stats
Since Last Clear
Packet Type          Sent  Received
Path                 1      0
Resv                 0      0
PathErr              0      0
RevErr               0      0
PathTear             0      0
ResvTear             0      0
ResvConf             0      0

Error
Since Last Clear
PATH state timeout    0
RESV state timeout    0

Rcv pkt proc error:  Since Last Clear
Path                 0      0
Resv                 0      0
PathErr              0      0
RevErr               0      0
PathTear             0      0
ResvTear             0      0
ResvConf             0      0

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to show the protocol statistics under the extensive option.</td>
</tr>
</tbody>
</table>
show mpls rsvp session p2mp

Displays Reserved Reservation Protocol (RSVP) point-to-multipoint sessions.

Syntax

show mpls rsvp session p2mp [ brief | detail | down | egress | extensive | in-interface | ingress | name | out-interface | p2mp-id | prepend | s2l | transit | up | wide ]

Parameters

brief
Displays brief session information.

detail
Displays detailed session information.

down
Displays inactive session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name. Some vendors allow each S2L sub-LSP for a P2MP LSP to have a different name. With such configurations in place the name filter responds in two different ways based on what other filters are applied in conjunction to the name filter.

- When the name filter is applied with p2mp filter and without and s2l filter, the entire P2MP session displays with all the S2L sub-LSPs in the detail format by default even if one of the S2L sub-LSP name matches with the supplied name in the CLI.
- When the name filter is applied with both p2mp filter and s2l filter, only that S2L-sub LSP whose name matches the name supplied displays along with the P2MP session’s common information in detail format.
- When name filter is applied with out-interface filter, only that S2L which matches both criteria displays.
- By default, in the common part of the P2MP session information, the name displayed would be the name of the first S2L-sub LSP displays in the detail format when no s2l filter is applied.

out-interface
Displays RSVP sessions going out on an interface. The out-interface filter would filter and display only those p2mp S2Ls that are going out via the interface requested. Other S2Ls not going out of the interface requested would not be displayed. The part common to all the S2Ls for a P2MP LSP displays first in the detail format followed by the S2L information.
p2mp-id
P2MP ID. It is the IP address picked from PE1 (Ingress), which could be same for multiple P2MP sessions originating from PE1. The P2MP ID is not a loopback address and may be any 32 bit number. The P2MP ID can also be local IP address. The P2MP-ID can be in Ip address or decimal format.

ppend
Displays sessions in soft preemption pending state.

s21
Displays point to multipoint source to leaf sub-LSPs.

transit
Displays transit session.

up
Displays UP session.

wide
Displays long LSP names.

Modes
User EXEC mode

Usage Guidelines

Examples
The following example displays the output of the command.

device# show mpls rsvp session p2mp
Total Number of such sessions are: 2
Ingress RSVP: 0 session(s)
Transit RSVP: 2 session(s)
P2MP_Id  From  Tunnel_Id  Style  Lbl_In  Num_S2l  LSPname
10.10.10.1  7.7.7.6  45  SE  1037  3  to-pe2
10.10.10.1  5.5.5.1  43  FF  3021  1  to-nyc
Egress RSVP: 0 session(s)
The following example displays the command with the wide option.

device# show mpls rsvp session p2mp s2l wide

Codes: DI: Ingress Detour  DT: Transit Detour  DM: Merged Detour
       DE: Egress Detour  BI: Ingress Backup  BM: Merged Backup  BE: Egress Backup
       RP: Repaired Session  BYI: Bypass Ingress

Total Number of such sessions are: 2

Ingress RSVP: 0 session(s)
Transit RSVP: 2 session(s)

<table>
<thead>
<tr>
<th>P2MP_ID</th>
<th>From</th>
<th>Tunnel_ID</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Num_S2L</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>7.7.7.6</td>
<td>45</td>
<td>SE</td>
<td>1037</td>
<td>3</td>
<td>to-pe2</td>
</tr>
</tbody>
</table>

To

<table>
<thead>
<tr>
<th>From</th>
<th>St Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out_Id</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>92.92.94.48</td>
<td>Up SE</td>
<td>1037</td>
<td>1028</td>
<td>ve101</td>
<td>to-pe2</td>
</tr>
<tr>
<td>92.92.95.48</td>
<td>Up SE</td>
<td>1037</td>
<td>1028</td>
<td>ve101</td>
<td>to-pe3</td>
</tr>
<tr>
<td>92.92.96.48</td>
<td>Up SE</td>
<td>1037</td>
<td>1028</td>
<td>ve101</td>
<td>to-pe4</td>
</tr>
</tbody>
</table>

The following example displays the command using the option P2MP-ID. The P2MP-ID can be in IP address or decimal format.

device# show mpls rsvp session p2mp p2mp-id 168430081

Total Number of such sessions are: 1

Ingress RSVP: 0 session(s)
Transit RSVP: 1 session(s)

<table>
<thead>
<tr>
<th>P2MP_ID</th>
<th>From</th>
<th>Tunnel_ID</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Num_S2L</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>168430081</td>
<td>7.7.7.6</td>
<td>45</td>
<td>SE</td>
<td>1037</td>
<td>3</td>
<td>to-pe2</td>
</tr>
</tbody>
</table>

Egress RSVP: 0 session(s)

device# show mpls rsvp session p2mp p2mp-id 20.0.0.1

Total Number of such sessions are: 1

Ingress RSVP: 0 session(s)
Transit RSVP: 1 session(s)

<table>
<thead>
<tr>
<th>P2MP_ID</th>
<th>From</th>
<th>Tunnel_ID</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Num_S2L</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>7.7.7.6</td>
<td>45</td>
<td>SE</td>
<td>1037</td>
<td>3</td>
<td>to-pe2</td>
</tr>
</tbody>
</table>

Egress RSVP: 0 session(s)
The following example displays the output of the command with the detail option. The first part of the command displays the attributes and information that are common to all S2Ls of the P2MP LSP. The second part displays information about each of the individual S2L sub LSP. In this output, there are two S2Ls for the session.

device# show mpls rsvp session p2mp detail

Total Number of such sessions are: 1

<table>
<thead>
<tr>
<th>P2MP_Id</th>
<th>From</th>
<th>Tunnel_Id</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Num_S2L</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>7.7.7.6</td>
<td>45</td>
<td>SE</td>
<td>1037</td>
<td>3</td>
<td>to-pe2</td>
</tr>
</tbody>
</table>

Tspspec: peak 1 kbps rate 1 kbps size 0 bytes m 20 M 65535
Setup Priority: 7 Holding Priority: 0
Session attribute flags:0x04(SE Style)

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>St</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out_If</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>92.92.94.48</td>
<td>7.7.7.6</td>
<td>Up</td>
<td>SE</td>
<td>1037</td>
<td>1028</td>
<td>ve101</td>
<td>to-pe2</td>
</tr>
</tbody>
</table>

LSP ID: 2, Sub-group Originator ID: 7.7.7.6 Sub-group ID: 2
Time left in seconds (PATH refresh: 0, ttd: 133
RESV refresh: 0, ttd: 156)
Explicit path hop count: 2
7.1.13.2 (S) -> 21.21.21.1 (S) -> 31.31.31.1(S)
Received RRO count: 2
Protection codes/Rtr Id flag: P: Local N: Node B: Bandwidth I: InUse R: RtrId
PATH rcvfrom: 7.1.18.2 (e4/1) (MD5 OFF), Message ID: 75
PATH sentto: 7.1.13.2 (ve101) (MD5 OFF), Message ID: 2575
RESV rcvfrom: 7.1.13.2 (ve101) (MD5 OFF), Message ID: 54024

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>St</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out_If</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>92.92.95.48</td>
<td>7.7.7.6</td>
<td>Up</td>
<td>SE</td>
<td>1037</td>
<td>1028</td>
<td>ve101</td>
<td>to-pe3</td>
</tr>
</tbody>
</table>

LSP ID: 2, Sub-group Originator ID: 7.1.18.2 Sub-group ID: 2
Time left in seconds (PATH refresh: 0, ttd: 153
RESV refresh: 0, ttd: 121)
Explicit path hop count: 3
7.1.13.2 (S) -> 21.21.21.1 (S) -> 41.41.41.1 (S)
Received RRO count: 3
Protection codes/Rtr Id flag: P: Local N: Node B: Bandwidth I: InUse R: RtrId
7.1.13.2 -> 21.21.21.1 -> 41.41.41.1
PATH rcvfrom: 7.1.18.2 (e4/1) (MD5 OFF), Message ID: 77
PATH sentto: 7.1.13.2 (ve101) (MD5 OFF), Message ID: 2577
RESV rcvfrom: 7.1.13.2 (ve101) (MD5 OFF), Message ID: 54026

<SNIPPED output for 3rd S2L>

Egress RSVP: 0 session(s)
show mpls rsvp session p2p
Displays Reserved Reservation Protocol (RSVP) point-to-point sessions.

Syntax
show mpls rsvp session p2p [ backup | brief | bypass | destination | detail | detour | down | egress | extensive | in-interface | ingress | name | out-interface | ppend | transit | up | wide ]

Parameters
backup
Displays facility backup session information.
brie
Displays brief session information.
bypass
Displays bypass session.
destination
Destination IP address.
detail
Displays detailed session information.
detour
Displays detour session.
down
Displays inactive session.
egress
Displays egress session.
extensive
Displays extensive session information.
in-interface
Displays RSVP sessions coming into an interface.
ingress
Displays ingress session.
name
Displays session by name.
out-interface
Displays RSVP sessions going out on an interface.
ppend
Displays sessions in a soft preemption pending state.
transit
Show Commands

Displays transit session.

up
Displays UP session.

wide
Displays long LSP names.

Modes
User EXEC mode

Usage Guidelines

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to include the P2P option.</td>
</tr>
</tbody>
</table>
show mpls rsvp session ppend

Displays Reserved Reservation Protocol (RSVP) sessions that are in a soft preemption state.

Syntax

show mpls rsvp session ppend [ brief | destination | detail | down | egress | extensive | in-interface | ingress | name | out-interface | p2mp | p2p | transit | up | wide ]

Parameters

brief
Displays brief session information.

destination
Destination IP address.

detail
Displays detailed session information.

down
Displays inactive session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint session.

p2p
Displays point to point session.

transit
Displays transit session.

up
Displays Up session.

wide
Displays long LSP names.

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays the appended view of the session.

device(config-mpls-lsp-high)#show mpls rsvp sess ppend
Codes: DI:Ingress Detour DT:Transit Detour DM:Merged Detour
DE:Egress Detour BI:Ingress Backup BM: Merged Backup BE:Egress Backup
RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 1

Transit RSVP: 1 session(s)
To     From     St Style Lbl_In Lbl_Out Out_If LSPname
80.80.80.80  40.40.40.40  Up SE  1024   3  e1/7   1
show mpls rsvp session transit
Displays Reserved Reservation Protocol (RSVP) transit sessions.

Syntax
show mpls rsvp session transit [ backup | brief | destination | detail | detour | down | extensive | in-interface | name | out-interface | p2mp | p2p | ppend | statistics | up | wide ]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

destination
Destination IP address.

detail
Displays detailed session information.

detour
Displays detour session.

down
Displays inactive session.

extensive
Displays extensive session information.

in-interface
Displays RSVP session coming into an interface.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions on a soft preemption pending state.

statistics
Displays transit LSP traffic statistics.

up
Displays UP session.

**wide**

Displays long LSP names.

**Modes**

User EXEC mode

**Usage Guidelines**

**Examples**

The following example displays when at least one LP does not support all three statistics.

device# show mpls rsvp session transit statistics
* means statistics collection is not supported on one or more of the line cards

Total Number of such sessions are: 4

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>Packets</th>
<th>Bytes</th>
<th>Rate(kbps)</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>150.150.150.10</td>
<td>190.190.190.9</td>
<td>1007</td>
<td>7654903*</td>
<td>53556*</td>
<td>test1</td>
</tr>
<tr>
<td>150.150.150.10</td>
<td>190.190.190.9</td>
<td>0</td>
<td>0*</td>
<td>0*</td>
<td>test2</td>
</tr>
</tbody>
</table>

The following example displays when all of the LPs support all three statistics.

device# show mpls rsvp session transit statistics
* means statistics collection is not supported on one or more of the line cards

Total Number of such sessions are: 4

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>Packets</th>
<th>Bytes</th>
<th>Rate(kbps)</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>150.150.150.10</td>
<td>190.190.190.9</td>
<td>1007</td>
<td>7654903</td>
<td>53556</td>
<td>test1</td>
</tr>
<tr>
<td>150.150.150.10</td>
<td>190.190.190.16</td>
<td>626241</td>
<td>56255</td>
<td>485</td>
<td>test2</td>
</tr>
<tr>
<td>150.150.150.10</td>
<td>190.190.190.9</td>
<td>65946</td>
<td>35648469</td>
<td>63582</td>
<td>test3</td>
</tr>
<tr>
<td>150.150.150.10</td>
<td>190.190.190.9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>test4</td>
</tr>
</tbody>
</table>

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was modified to include the keyword &quot;statistics&quot;.</td>
</tr>
</tbody>
</table>
show mpls rsvp session up

Displays the number of UP Reserved Reservation Protocol (RSVP) sessions.

Syntax

show mpls rsvp session up [ backup | brief | bypass | destination | detail | detour | egress | extensive | in-interface | ingress | name | out-interface | p2mp | p2p | ppend | transit | wide ]

Parameters

backup
Displays facility backup session.

brief
Displays brief session information.

bypass
Displays bypass session.

destination
Destination IP address.

detail
Displays details session information.

detour
Displays detour session.

egress
Displays egress session.

extensive
Displays extensive session information.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending status.

transit

Displays transit session.

wide

Displays long LSP names.

**Modes**

User EXEC mode

**Usage Guidelines**

**Examples**

The following example displays the command using the wide option.

```
device#show mpls rsvp session up wide
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
      DE:Egress Detour  BI:Ingress Backup  BM: Merged Backup  BE:Egress Backup
      RP:Repaired Session  BYI: Bypass Ingress

Total Number of such sessions are: 59946
Transit RSVP: 59439 session(s)
```

<table>
<thead>
<tr>
<th>To</th>
<th>From</th>
<th>St</th>
<th>Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out If</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.20.1</td>
<td>172.16.50.1</td>
<td>Up</td>
<td>SE</td>
<td>58368</td>
<td>3</td>
<td>e15/2</td>
<td>LSP-63301</td>
</tr>
<tr>
<td>172.16.22.1</td>
<td>172.16.30.1</td>
<td>Up</td>
<td>SE</td>
<td>15873</td>
<td>23328</td>
<td>e21/6</td>
<td>LSP-10002</td>
</tr>
<tr>
<td>172.16.22.1</td>
<td>172.16.32.1(BI)</td>
<td>Up</td>
<td>-</td>
<td>15873</td>
<td>45255</td>
<td>e1/2</td>
<td>LSP-10002</td>
</tr>
<tr>
<td>172.16.22.1</td>
<td>172.16.30.1</td>
<td>Up</td>
<td>SE</td>
<td>54733</td>
<td>49673</td>
<td>e15/1</td>
<td>LSP-10003</td>
</tr>
<tr>
<td>172.16.22.1</td>
<td>172.16.32.1(BI)</td>
<td>Up</td>
<td>-</td>
<td>54733</td>
<td>43841</td>
<td>e1/2</td>
<td>LSP-10003</td>
</tr>
<tr>
<td>172.16.22.1</td>
<td>172.16.30.1</td>
<td>Up</td>
<td>SE</td>
<td>19472</td>
<td>15317</td>
<td>e1/8</td>
<td>LSP-10006</td>
</tr>
<tr>
<td>172.16.22.1</td>
<td>172.16.32.1(BI)</td>
<td>Up</td>
<td>-</td>
<td>19472</td>
<td>15317</td>
<td>e1/2</td>
<td>LSP-10006</td>
</tr>
</tbody>
</table>
show mpls rsvp session wide

Displays Reserved Reservation Protocol (RSVP) sessions with long LSP names.

Syntax

show mpls rsvp session wide [ backup | bypass | destination | detour | down | egress | in-interface | ingress | name | out-interface | p2mp | p2p | ppend | transit | up ]

Parameters

backup
Displays facility backup session.

bypass
Displays bypass session.

destination
Destination IP address.

detour
Displays detour session.

down
Displays inactive session.

egress
Displays egress session.

in-interface
Displays RSVP sessions coming into an interface.

ingress
Displays ingress session.

name
Displays session by name.

out-interface
Displays RSVP sessions going out on an interface.

p2mp
Displays point to multipoint sessions.

p2p
Displays point to point sessions.

ppend
Displays sessions in a soft preemption pending status.

transit
Displays transit session.

up
Displays UP session.

**Modes**

User EXEC mode

**Usage Guidelines**

**Examples**

The following example displays the output of the command.

```bash
device#show mpls rsvp session wide
```

Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour  
DE:Egress Detour  BI:Ingress Backup  BM: Merged Backup  
BE:Egress Backup  RP:Repaired Session  BYI: Bypass Ingress

Total Number of such sessions are: 1611

<table>
<thead>
<tr>
<th>Ingress RSVP</th>
<th>1088 session(s)</th>
<th>St Style</th>
<th>Lbl_In</th>
<th>Lbl_Out</th>
<th>Out_If</th>
<th>LSPname</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve207</td>
<td>to-nakul-156-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve205</td>
<td>to-nakul-179-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up FF</td>
<td>-</td>
<td>3</td>
<td>ve225</td>
<td>to-nakul-4</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve218</td>
<td>to-nakul-17-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve209</td>
<td>to-nakul-8-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve206</td>
<td>to-nakul-55-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve216</td>
<td>to-nakul-40-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve220</td>
<td>to-nakul-194-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve204</td>
<td>to-nakul-78-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve213</td>
<td>to-nakul-212-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve217</td>
<td>to-nakul-141-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve215</td>
<td>to-nakul-164-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve223</td>
<td>to-nakul-197-3.3.3.1</td>
</tr>
<tr>
<td>3.3.3.1</td>
<td>2.2.2.1</td>
<td>Up SE</td>
<td>-</td>
<td>3</td>
<td>ve225</td>
<td>to-nakul-174-3.3.3.1</td>
</tr>
</tbody>
</table>

device#

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.00</td>
<td>This command was modified to include the wide option. This option displays the full LSP name on a single line.</td>
</tr>
</tbody>
</table>
show mpls rsvp statistics

Displays the RSVP control packet statistics combined over all the interfaces.

**Syntax**

```
show mpls rsvp statistics
```

**Modes**

User EXEC mode

**Usage Guidelines**

The device constantly gathers RSVP statistics. RSVP statistics are collected from the time RSVP is enabled, as well as from the last time the RSVP statistics counters were cleared.

The command resets the counters listed under the ‘Since last clear’ column for the `show mpls rsvp interface detail` and `show mpls rsvp statistics` commands.

This command operates in all modes.

**Command Output**

The `show mpls rsvp statistics` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>The number of Path messages sent and received. Path messages store information about the state of the path along the LSRs in the LSP.</td>
</tr>
<tr>
<td>Resv</td>
<td>The number of RESV messages sent and received. RESV messages include Fixed Filter (FF), Wildcard Filter (WF), and Shared Explicit (SE) messages.</td>
</tr>
<tr>
<td>PathErr</td>
<td>The number of PathErr messages sent and received.</td>
</tr>
<tr>
<td>ResvErr</td>
<td>The number of ResvErr messages sent and received.</td>
</tr>
<tr>
<td>PathTear</td>
<td>The number of PathTear messages sent and received. PathTear messages cause path states to be deleted.</td>
</tr>
<tr>
<td>ResvTear</td>
<td>The number of ResvTear messages sent and received. ResvTear messages cause reservation states to be deleted.</td>
</tr>
<tr>
<td>ResvConf</td>
<td>The number of reservation confirmation messages sent and received.</td>
</tr>
<tr>
<td>Rcv pkt bad length</td>
<td>The number of times a packet was not processed because it was the wrong length.</td>
</tr>
<tr>
<td>Rcv pkt unknown type</td>
<td>The number of times an RSVP packet was not processed because it was not one of the types defined in RFC 2205.</td>
</tr>
<tr>
<td>Rcv pkt bad version</td>
<td>The number of times a packet was not processed because it was an RSVP version other than one.</td>
</tr>
<tr>
<td>Rcv pkt bad cksum</td>
<td>The number of times a packet was not processed because of a bad RSVP checksum.</td>
</tr>
<tr>
<td>Memory alloc fail</td>
<td>The number of times a packet was not processed because RSVP memory allocation failed on the device.</td>
</tr>
</tbody>
</table>
### TABLE 10 Rcv pkt processing errors

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>The number of Path messages received with a packet processing error.</td>
</tr>
<tr>
<td>Resv</td>
<td>The number of RESV messages received with a packet processing error.</td>
</tr>
<tr>
<td>PathErr</td>
<td>The number of PathErr messages received with a packet processing error.</td>
</tr>
<tr>
<td>ResvErr</td>
<td>The number of ResvErr messages received with a packet processing error.</td>
</tr>
<tr>
<td>PathTear</td>
<td>The number of PathTear messages received with a packet processing error.</td>
</tr>
<tr>
<td>ResvTear</td>
<td>The number of reservation confirmation messages received with a packet processing error.</td>
</tr>
<tr>
<td>ResvConf</td>
<td>The number of reservation confirmation messages received with a packet processing error.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the `show mpls rsvp statistics` command output.

```console
device# show mpls rsvp statistics
Total Since last clear
PacketType Sent Received Sent Received
Path  4  4  4  4
Resv  4  4  4  4
PathErr 0  0  0  0
ResvErr 0  0  0  0
PathTear 0  0  0  0
ResvTear 0  0  0  0
ResvConf 0  0  0  0
Errors Total Since last clear
Rcv pkt bad length  0  0
Rcv pkt unknown type 0  0
Rcv pkt bad version 0  0
Rcv pkt bad cksum 0  0
Memory alloc fail 0  0
Rcv pkt processing error:
Path 0  0
Resv 0  0
PathErr 0  0
ResvErr 0  0
PathTear 0  0
ResvTear 0  0
ResvConf 0  0
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>The 'Hello' packet type was added. The <code>clear mpls rsvp statistics</code> command clears the 'since last clear' column for the 'Hello' packet type.</td>
</tr>
</tbody>
</table>
show mpls static-lsp
Displays the static LSPs in the system.

Syntax
- `show mpls static-lsp [ brief | debug | detail | wide ]`
- `show mpls static-lsp extensive [ descending ]`
- `show mpls static-lsp name lsp-name extensive [ descending ]`
- `show mpls static-lsp { down | up } [ detail | wide | extensive [ descending ] ]`

Parameters
- **brief**
  Displays brief information.
- **debug**
  Displays debug information, with history.
- **detail**
  Displays detailed information.
- **wide**
  Displays long LSP names.
- **extensive**
  Displays detailed information with History.
- **descending**
  Displays LSP History with newer entries on top.
- **name lsp-name**
  Displays information by LSP name.
- **down**
  Displays operationally DOWN LSPs.
- **detail**
  Displays detailed information of the operationally DOWN LSPs.
- **extensive**
  Displays detailed information with History of the operationally DOWN LSPs.
- **wide**
  Displays long LSP names of the operationally DOWN LSPs.
- **up**
  Displays operationally UP LSPs.

Modes
- User EXEC mode
Command Output

The `show mpls static-lsp` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the static LSP as configured by the user.</td>
</tr>
<tr>
<td>Admin</td>
<td>Whether or not the static LSP is enabled.</td>
</tr>
<tr>
<td>Oper</td>
<td>Operational state of the LSP.</td>
</tr>
<tr>
<td>In-label</td>
<td>The in-label configured for the LSP.</td>
</tr>
<tr>
<td>Out-label</td>
<td>The out-label configured. If none, the implicit-null label 3 is shown.</td>
</tr>
<tr>
<td>Next-hop</td>
<td>The configured next-hop.</td>
</tr>
<tr>
<td>Out-Intf</td>
<td>The out-interface that corresponds to the next-hop configured.</td>
</tr>
</tbody>
</table>

The `show mpls static-lsp extensive` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>The role of the LSP. Only transit.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the LSP is enabled or not.</td>
</tr>
<tr>
<td>Times LSP goes UP since enabled</td>
<td>Number of times the LSP has gone UP since being enabled.</td>
</tr>
<tr>
<td>In-label</td>
<td>The in-label configured for the LSP.</td>
</tr>
<tr>
<td>Next-hop</td>
<td>The configured next-hop.</td>
</tr>
<tr>
<td>History</td>
<td>The static-lsp sample History.</td>
</tr>
<tr>
<td>Static-LSP</td>
<td>Identifier of the static-LSP.</td>
</tr>
<tr>
<td>Role</td>
<td>The role of the LSP. Currently, only transit.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the LSP is enabled or not.</td>
</tr>
<tr>
<td>UP</td>
<td>Whether LSP is operational or not.</td>
</tr>
<tr>
<td>LSP error</td>
<td>Reason LSP is down or if there was any error during any processing on the LSP.</td>
</tr>
<tr>
<td>Times LSP goes UP since enabled</td>
<td>Number of times the LSP has gone UP since being enabled.</td>
</tr>
<tr>
<td>In-label</td>
<td>The in-label configured for the LSP.</td>
</tr>
<tr>
<td>Out-label</td>
<td>The configured out-label, three if implicit-null.</td>
</tr>
<tr>
<td>Next-hop</td>
<td>The configured next-hop.</td>
</tr>
<tr>
<td>Out-interface for the next-hop</td>
<td>The out-interface that corresponds to the configured next-hop.</td>
</tr>
<tr>
<td>Next-hop interface address to reach configured next-hop</td>
<td>The interface address to reach the next-hop address configured. It is the same as the configured next-hop in case the configured next-hop address is directly connected and different if not directly-connected.</td>
</tr>
</tbody>
</table>

Examples

The following example displays the output of the `show mpls static-lsp` command.

device# show mpls static-lsp
Number of transit lpsps: 2
Name  Admin  Oper  In-label Out-label  Next-hop          Out-Intf
  c2    UP     DOWN  21      1024    160.168.123.122     e2/1
  c3    UP     UP     22      3       160.168.111.100    ve10
The following example displays the output of the `show mpls static-lsp extensive` command.

device# show mpls static-lsp extensive
Static-LSP t1, Role: Transit
   Enabled: Yes, UP: Yes
   Times LSP goes up since enabled: 1
   In-label: 201, Out-label: 3,
   Next-hop: 120.120.120.2,
   Out-Interface for the next-hop: e2/1
   Next-hop interface address to reach configured next-hop: 10.1.1.2
   History
      0 Jul 11 01:38:32 : LSP tunnel is Enabled
      1 Jul 11 01:38:33 : Static Transit LSP UP
Static-LSP t2, Role: Transit
   Enabled: Yes, UP: No
   LSP error: No interface available for next-hop
   Times LSP goes up since enabled: 1
   In-label: 202, Out-label: 3,
   Next-hop: 20.1.1.2,
   Out-Interface for the next-hop: --
   Next-hop interface address to reach configured next-hop: --
   History
      0 Jul 11 01:38:32 : LSP tunnel is Enabled

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was modified to include the keyword “descending” to display the LSP History in reverse chronological order.</td>
</tr>
</tbody>
</table>
**show mpls statistics 6pe**

Displays IPv6 over MPLS statistics.

**Syntax**

```
show mpls statistics 6pe [ slot/port | vrf ]
```

**Parameters**

- `slot/port`  
  Displays MPLS statistics for the specified interface number.

- `vrf`  
  Displays statistics based on VRFs.

**Modes**

User EXEC mode

**Usage Guidelines**

This command operates in all modes.

The `clear mpls statistics 6pe slot/port` command clears the 6pe statistics.

**Examples**

The following example displays the number of 6PE packets going into or coming out of the MPLS cloud. The packet counter is per PPCR.

```plaintext
device# show mpls statistics 6pe
In-Port(s)       Endpt Out-Pkt            Tnl Out-Pkt
e2/1 - e2/4      0                    0
e2/5 - e2/8      0                    0
e4/1 - e4/2      41810353             0
e4/3 - e4/4      0                    41810352
device
```

The following example displays the number of IPv6 packets from a provider edge (PE) router going into or coming out of the MPLS cloud.

```plaintext
device> show mpls statistics 6pe
In-Port(s)       Endpt Out-Pkt            Tnl Out-Pkt
e1/1 - e1/2     184116072          1697803327
e1/3 - e1/4     389547885          6036111
e2/1 - e2/24    1088610            0
e2/25 - e2/48    0                  248406
e3/1            2045067126         5288598554
e3/2            0                  0
device
```
show mpls statistics bypass-lsp

Displays the incoming packet count and byte count rate (in bytes) on a tunnel interface for bypass LSPs.

Syntax

```
show mpls statistics bypass-lsp lsp-name
```

Parameters

`lsp-name`

The name of the specified LSP.

Modes

User EXEC mode

Examples

The following example shows the `show mpls statistics bypass-lsp lsp-name` command.

```
device# show mpls statistics bypass-lsp
   LSP B1
   Tunnel interface tnl4 100 pkt 2200 Byte Last Update Dec 17 18:51:21.000
   LSP B1
   Tunnel interface tnl6 900 pkt 33445 Byte Last Update Dec 17 18:51:38.000
   LSP B1
   Tunnel interface tnl9 78 pkt 7229 Byte Last Update Dec 17 18:51:41.000
   LSP B1
   Tunnel interface tnl15 456 pkt 2398 Byte Last Update Dec 17 18:52:1.000
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show mpls statistics label**

Displays statistics for LDP ECMP paths.

**Syntax**

```
show mpls statistics label
```

**Parameters**

`label`

Displays the in-label statistics.

**Modes**

User EXEC mode

**Usage Guidelines**

**Command Output**

The `show mpls statistics label` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-label</td>
<td>The MPLS label ID.</td>
</tr>
<tr>
<td>In-Port(s)</td>
<td>The port where the traffic arrives.</td>
</tr>
<tr>
<td>In-Packet Count</td>
<td>The number of packets meeting the In-label and In-port criteria.</td>
</tr>
<tr>
<td>In-Bytes Count</td>
<td>The number of bytes meeting the In-label and In-port criteria.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays all of the MPLS traffic statistics by their MPLS label.

```
device# show mpls statistics label
In-label In-Port(s) In-Packet Count
1024    e3/1       315431
        e3/2       349193
        e3/3       0
        e3/4       0
1025    e3/1       419750
        e3/2       0
        e3/3       0
        e3/4       0
1024    e5/1 - e5/10 364690
        e5/11 - e5/20 0
        e5/21 - e5/30 0
1025    e5/1 - e5/10 0
        e5/11 - e5/20 0
        e5/21 - e5/30 0
```
The following example displays all the MPLS traffic statistics by their MPLS label for a Brocade NetIron CES Series or Brocade NetIron CER Series device.

```
device# show mpls statistics label
In-label In-Port(s)  In-Bytes Count
1024    e1/1-e1/24    315431
         e1/25-e1/48    0
```

The following example displays all MPLS traffic statistics, by their MPLS label, which are gathered by the corresponding network processor.

```
device# show mpls statistics label 3/1
In-label      In-Port(s)     In-Packet Count
1024          e3/1 - e3/20    30
1026          e3/1 - e3/20    21
1030          e3/1 - e3/20    100
1032          e3/1 - e3/20    0
1033          e3/1 - e3/20    0
1034          e3/1 - e3/20    12
1036          e3/1 - e3/20    0
```

The following example displays all MPLS traffic statistics by their MPLS label for a specific port on a Brocade NetIron CES Series or Brocade NetIron CER Series device.

```
device# show mpls statistics label 1/1
In-label In-Port(s)  In-Bytes count
1024    e1/1-e1/24    315431
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.00</td>
<td>This command was modified to display statistics for LDP ECMP paths.</td>
</tr>
</tbody>
</table>
show mpls statistics ldp transit
Displays the traffic statistics for transit LDP FECs.

Syntax

```
show mpls statistics ldp transit [ fec ip-addr [/subnet-mask ] ]
```

Parameters

- **fec ip-addr**
  Displays the traffic statistics for the transit LDP FECs.

- **IP-subnet-mask**
  Specifies an IP subnet-mask length.

Modes

User EXEC mode

Usage Guidelines

This command operates in all modes.

Packet count is not available for Brocade NetIron CES Series and Brocade NetIron CER Series devices.

Command Output

The `show mpls statistics ldp transit` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEC</td>
<td>The specified FEC for MPLS LDP transit statistics.</td>
</tr>
<tr>
<td>Packets</td>
<td>Specifies the number of packets received.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Specifies the number of bytes received.</td>
</tr>
<tr>
<td>Rate-kbps</td>
<td>Rate is in kilobits per second.</td>
</tr>
</tbody>
</table>

Examples

The following example displays output from the `show mpls statistics ldp transit` command:

```
device# show mpls statistics ldp transit
FEC     Packets  Bytes     Rate-kbps
10.35.0/30      0   0*        0*
10.35.10.1/32    0   0*        0*
10.255.245.214/32 112 7566182* 6224*
192.168.37.36/30 532114 2350644* 564*
```

* means statistics collection is not supported on one or more of the line cards.
The following example displays output from the `show mpls statistics transit` command with the `fec` keyword:

```
device# show mpls statistics ldp transit fec 10.255.245.214
FEC         Packets  Bytes      Rate-kbps
10.255.245.214/32 112    7566182*  6224*
```

* means statistics collection is not supported by one or more of the line cards.

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command is modified to include the parameters <code>transit</code>, <code>fec</code>, and <code>ip_addr</code>.</td>
</tr>
</tbody>
</table>
**show mpls statistics ldp tunnel**
Displays the total combined statistics of all ECMP paths of an LDP tunnel with LDP ECMP LER feature.

**Syntax**
```
show mpls statistics ldp tunnel [ dec | vif-index ]
```

**Parameters**
- **dec**
  Specifies the destination prefix.
- **vif-index**
  Displays the total combined statistics of all ECMP paths of an LDP tunnel with LDP ECMP LER feature.

**Modes**
User EXEC mode

**Usage Guidelines**
The statistics are not accurate when the system runs out of CAM entries for all the ECMP paths.

**Command Output**
The `show mpls statistics ldp tunnel` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>The name of the LSP that statistics are being displayed for (displayed for RSVP-signaled LSPs only).</td>
</tr>
<tr>
<td>tnl</td>
<td>The index number of the MPLS tunnel</td>
</tr>
<tr>
<td>pkt</td>
<td>The total number of packets forwarded through the specified LSP.</td>
</tr>
<tr>
<td>Byte</td>
<td>The total number of bytes forwarded through the specified LSP.</td>
</tr>
<tr>
<td>Avg. pps</td>
<td>The number of packets-per-second forwarded through the specified LSP.</td>
</tr>
<tr>
<td>Avg. Bps</td>
<td>The number of bytes-per-second forwarded through the specified LSP.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows the output of the `show mpls statistics ldp tunnel` command.
```
device# show mpls statistics ldp tunnel
LDP tunnel interface tn113  0 pkt  0 Byte  0 Avg. pps  0 Avg. Bps
```

**History**

<table>
<thead>
<tr>
<th>Release Version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to show the total combined statistics of all ECMP paths of an LDP tunnel with the LDP ECMP LER feature.</td>
</tr>
</tbody>
</table>
show mpls statistics lsp

Displays ingress tunnel accounting for RSVP-signaled LSPs.

Syntax

```
show mpls statistics lsp [ lsp_name ]
```

Parameters

<table>
<thead>
<tr>
<th>lsp_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays statistics for a specified LSP.</td>
</tr>
</tbody>
</table>

Modes

User EXEC mode

Usage Guidelines

Examples

The following example displays output from the `show mpls statistics lsp` command:

```
device# show mpls statistics lsp
LSP topo4
   Tunnel index 0 0 pkt 0 Byte 0 Avg. pps 0 Avg. Bps
LSP 400
   Tunnel index 2 0 pkt 0 Byte 0 Avg. pps 0 Avg. Bps
LSP 4000
   Tunnel index 3 0 pkt 0 Byte 0 Avg. pps 0 Avg. Bps
LSP topo41
   Tunnel index 4 99205408 pkt 11314220016 Byte 84459 pps 9628340 Bps
```
show mpls statistics oam
Displays OAM MPLS statistics.

Syntax
show mpls statistics oam

Modes
User EXEC mode.

Usage Guidelines
Use the show mpls statistics oam command to display the following LSP ping and traceroute counters:

- Ping and traceroute requests that are issued by the user
- Echo requests sent
- Echo requests received
- Echo request time-outs
- Echo replies sent
- Echo replies received
- Echo replies with error return codes

The clear mpls statistics oam command clears the LSP ping and traceroute counters.

Examples
The following example displays the output of the show mpls statistics oam command.

device # show mpls statistics oam
User ping request processed: 8
User traceroute request processed: 3
Echo requests: sent(102658), received(2865), timeout(0)
Echo replies: sent(2865), received(102628)
Echo reply return code distribution: TX RX
Egress(3) : 0 102628
Transit(8) : 0 0
No return code(0) : 0 0
Malformed request(1) : 0 0
Unsupported TLV(2) : 2865 0
No FEC mapping(4) : 0 0
DS map mismatch(5) : 0 0
Unknown upstream intf(6) : 0 0
Reserved return code(7) : 0 0
Unlabeled output intf(9) : 0 0
FEC mapping mismatch(10) : 0 0
No label entry(11) : 0 0
Rx intf protocol mismatch(12) : 0 0
Premature LSP termination(13) : 0 0
show mpls statistics vll

Displays VLL endpoint traffic statistics to see the forwarding counters for each VLL configured on the system.

Syntax

```
show mpls statistics vll [ vll-id extended-counters | vll-name extended-counters ]
```

Parameters

- **vll-id**
  - Specifies the identifier of a VLL instance.
- **vll-name**
  - Specifies the configured name for a VLL instance.
- **extended-counters**
  - Displays extended counter (Generation 2 and 3a modules only).

Modes

User EXEC mode.

Command Output

The `show mpls statistics vll` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLL-Name</td>
<td>The configured name of the VLL instance.</td>
</tr>
<tr>
<td>VLL-Ports</td>
<td>The port where the traffic is monitored.</td>
</tr>
<tr>
<td>VLL-ingress-Pkts</td>
<td>Packets arriving from the Customer Endpoint.</td>
</tr>
<tr>
<td>VLL-Egress-Pkts</td>
<td>Packets arriving from the MPLS core and going to the customer interface.</td>
</tr>
</tbody>
</table>

Examples

The following example displays output of all VLL traffic statistics on a Brocade device.

```
device# show mpls statistics vll

VLL-Name    VLL-Ports    VLL-Ingress-Pkts    VLL-Egress-Pkts
--------    ---------    ----------------    ---------------
VLL1        e1/1         100                 100
VLL2        e1/4         100                 100
```

**NOTE**

The VLL name repeats for each module where the statistics are collected and display on the Management console.

The following example shows the output of VLL traffic statistics for a VLL instance, specified by its VLL name.

```
device# show mpls statistics vll vll1

VLL-Name    VLL-Ports    VLL-Ingress-Pkts    VLL-Egress-Pkts
--------    ---------    ----------------    ---------------
VLL1        e1/1         100                 100
```
The following example shows the output of VLL traffic statistics for a VLL specified by its VLL ID.

device# show mpls statistics vll 4

<table>
<thead>
<tr>
<th>VLL-Name</th>
<th>VLL-Ports</th>
<th>VLL-Ingress-Pkts</th>
<th>VLL-Egress-Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLL1</td>
<td>e1/1</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>
**show mpls statistics vll-local**

When extended counters are enabled, displays the number of bytes and packets received and sent on a particular endpoint or all endpoints of that Local VLL instance.

**Syntax**

```
show mpls statistics local-vll [vll_name | vll_id [extended-counters [ [ vlan vlan_id ] [ ethernet port_id ] ] ]]
```

**Parameters**

- `vll_name`  
  Specifies the configured name for the Local VLL instance.

- `vll_id`  
  Specifies the ID of a Local VLL instance.

- `extended-counters`  
  Enables the extend counters for a particular Local VLL instance.

- `vlan vlan_id`  
  Specifies the ID of the configured VLAN.

- `ethernet port_id`  
  Specifies the Ethernet port.

**Modes**

User EXEC mode.

**Usage Guidelines**

`clear mpls statistics vll-local`

**Command Output**

The `show mpls statistics vll-local` command with the `extended-counters` option displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLL</td>
<td>The configured name for a Local VLL instance.</td>
</tr>
<tr>
<td>VLL-ID</td>
<td>The ID of the Local VLL instance.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The ID of the configured VLAN.</td>
</tr>
<tr>
<td>Port</td>
<td>The port ID of the interface for which the user wants to display the counters.</td>
</tr>
<tr>
<td>RxPkts</td>
<td>The number of packets received at the specified port.</td>
</tr>
<tr>
<td>TxPkts</td>
<td>The number of packets transmitted from the specified port.</td>
</tr>
<tr>
<td>RxBytes</td>
<td>The number of bytes received at the specified port.</td>
</tr>
<tr>
<td>TxBytes</td>
<td>The number of bytes transmitted from the specified port.</td>
</tr>
</tbody>
</table>
Examples

The following example displays the output of the `show mpls statistics vll-local` command with the `extended-counters` option:

```
device# show mpls statistics vll-local loc8 extended-counters
VLL loc8, VLL-ID9:Extended Counters (only applicable for G2 modules)
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Port</th>
<th>RxPkts</th>
<th>TxPkts</th>
<th>Rxbytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>94</td>
<td>5/2</td>
<td>4639941</td>
<td>0</td>
<td>1187824896</td>
<td>0</td>
</tr>
<tr>
<td>p0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>p1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>p2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>p3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>p4</td>
<td>0</td>
<td>4639941</td>
<td>0</td>
<td>1187824896</td>
<td>0</td>
</tr>
<tr>
<td>p5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>p6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>p7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

When the per-VLAN, port, and priority-based accounting mode is disabled, the following output is displays for the `show mpls statistics vll-local` command with the `extended-counters` option:

```
device# show mpls statistics vll-local loc8 extended-counters
VLL loc8, VLL-ID9:Extended Counters (only applicable for G2 modules)
<table>
<thead>
<tr>
<th>VLAN</th>
<th>Port</th>
<th>RxPkts</th>
<th>TxPkts</th>
<th>Rxbytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>94</td>
<td>5/2</td>
<td>1175769</td>
<td>0</td>
<td>300996864</td>
<td>0</td>
</tr>
<tr>
<td>92</td>
<td>8/2</td>
<td>0</td>
<td>1178559</td>
<td>0</td>
<td>301711104</td>
</tr>
</tbody>
</table>
```
show mpls statistics vpls
     Displays statistics based on VPLSs.

Syntax

show mpls statistics vpls [ vpls_id | vpls_name ]
show mpls statistics vpls [ vpls_id | vpls_name ] extended-counters vlan vlan_id [ detail | routed | switched ]
show mpls statistics vpls [ vpls_id | vpls_name ] extended-counters vlan vlan_id [ inner-vlan inner_vlan_id ] [ ethernet slot / port ] [ detail | routed | switched ]

Parameters

vpls_id
    Displays specified VPLS by numerical ID.

vpls_name
    Displays specified VPLS by name.

vlan vlan_id
    Displays Extended Counters for end points of a VPLS VLAN (single tag only).

extended-counters
    Displays Extended Counters (G2/G3 modules only).

detail
    Displays Extended Counters in a detailed format.

routed
    Displays Extended Counters for routed packets.

switched
    Displays Extended Counters for switched packets.

inner-vlan inner_vlan_id
    Specifies the ID of the configured inner VLAN.

ethernet slot / port
    Displays Extended Counters for a VPLS endpoint.

Modes

User EXEC mode
Usage Guidelines

Examples

The following example displays the `show mpls statistics vpls` command with the `extended-counters detail` option.

device#show mpls statistics vpls 1 extended-counters detail
VPLS Extended Counters (only applicable for G2 modules): VPLS Name: a, VPLS Id: 1

<table>
<thead>
<tr>
<th>VPLS Vlan: vlan 100</th>
<th>Interface RxPkts</th>
<th>TxPkts</th>
<th>RxBytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth 4/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routed 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Switched 6525316</td>
<td>15195085</td>
<td>574227808</td>
<td>1337167480</td>
<td></td>
</tr>
<tr>
<td>Combined 6525316</td>
<td>15195085</td>
<td>574227808</td>
<td>1337167480</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VPLS Vlan: vlan 200</th>
<th>Interface RxPkts</th>
<th>TxPkts</th>
<th>RxBytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth 4/8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routed 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Switched 17084263</td>
<td>5845698</td>
<td>1503415144</td>
<td>514421424</td>
<td></td>
</tr>
<tr>
<td>Combined 17084263</td>
<td>5845698</td>
<td>1503415144</td>
<td>514421424</td>
<td></td>
</tr>
</tbody>
</table>

The following example displays the `show mpls statistics vpls` command with the `extended-counters routed` option.

device#show mpls statistics vpls 1 extended-counters routed
VPLS Extended Counters (only applicable for G2 modules): VPLS Name: a, VPLS Id: 1

<table>
<thead>
<tr>
<th>VPLS Vlan: vlan 100</th>
<th>Interface RxPkts</th>
<th>TxPkts</th>
<th>RxBytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth 4/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routed 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VPLS Vlan: vlan 200</th>
<th>Interface RxPkts</th>
<th>TxPkts</th>
<th>RxBytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth 4/8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following example displays the `show mpls statistics vpls` command with the `extended-counters switched` option.

device#show mpls statistics vpls 1 extended-counters switched
VPLS Extended Counters (only applicable for G2 modules): VPLS Name: a, VPLS Id: 1

<table>
<thead>
<tr>
<th>VPLS Vlan: vlan 100</th>
<th>Interface RxPkts</th>
<th>TxPkts</th>
<th>RxBytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth 4/1</td>
<td>6525316</td>
<td>15195085</td>
<td>574227808</td>
<td>1337167480</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VPLS Vlan: vlan 200</th>
<th>Interface RxPkts</th>
<th>TxPkts</th>
<th>RxBytes</th>
<th>TxBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth 4/8</td>
<td>17084263</td>
<td>5845698</td>
<td>1503415144</td>
<td>514421424</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was modified to display MPLS routed and switched statistics. Use this command to get statistics per VLAN and per interface, either routed or switched. This is available for only Gen2 cards.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the <code>inner-vlan vlan_id</code> parameter.</td>
</tr>
</tbody>
</table>
show mpls statistics vrf

Displays statistics based on Virtual Routing and Forwarding (VRF)s.

Syntax

show mpls statistics vrf vrf_name

Parameters

vrf_name

Displays specified VRF by name.

Modes

User EXEC mode

Usage Guidelines

Command Output

The `show mpls statistics vrf` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF Name</td>
<td>The name of the VRF from which packets originated or are destined.</td>
</tr>
<tr>
<td>In-Port(s)</td>
<td>The port that is either the VRF or MPLS interface.</td>
</tr>
<tr>
<td>Endpt Out-Pkt</td>
<td>The number of packets forwarded to the specified VRF interface.</td>
</tr>
<tr>
<td>Tnl Out-Pkt</td>
<td>The number of VRF data packets sent to the remote peer over an MPLS tunnel.</td>
</tr>
</tbody>
</table>
**Examples**

The following example displays out-packet statistics for VRFs.

```plaintext
device# show mpls statistics vrf
VRF Name In-Port(s) Endpt Out-Pkt Tnl Out-Pkt
red  e3/1  0  0
e3/2  0  0
e3/3  0  0
e3/4  0  0
e5/1 - e5/10  0  0
e5/11 - e5/20  0  0
e5/21 - e5/30  0  0
e5/31 - e5/40  0  0
green e3/1  3707480  0
e3/2  2692915  0
e3/3  0  0
e3/4  0  0
e5/1 - e5/10  0  0
e5/11 - e5/20  0  5834179
e5/21 - e5/30  0  0
e5/31 - e5/40  0  0
pink  e3/1  0  0
e3/2  0  0
e3/3  0  0
e3/4  0  0
e5/1 - e5/10  0  0
e5/11 - e5/20  0  0
e5/21 - e5/30  0  0
e5/31 - e5/40  0  0
```

The following example displays out-packet statistics for a specific VRF.

```plaintext
device# show mpls statistics vrf black
VRF Name In-Port(s) Endpt Out-Pkt Tnl Out-Pkt
black e3/1  0  0
e3/2  29607351  0
e3/3  27522998  25828420
e3/4  0  0
e5/1 - e5/10  0  0
e5/11 - e5/20  0  0
e5/21 - e5/30  0  0
e5/31 - e5/40  0  0
```

**show mpls summary**

Displays a summary of MPLS information, including the number of configured paths and signaled LSPs for which this device is the ingress LSR.

**summary**

- Displays MPLS global counters.

**User EXEC mode**

The `show mpls summary` command output has additional information on the total number of bypass LSPs in the system. This total number is the sum of the configured static and dynamic bypasses in the system.

The `show mpls summary` command displays the following information:
The following example displays the output of the `show mpls summary` command.

device# show mpls summary
CER40 (config-mpls-lsp-test)#show mpls summary

Path:
  Paths configured - 2

RSVP-Signaled LSPs:
  LSPs configured - 6
  LSPs enabled - 6
  LSPs operational - 6
  Detour LSPs UP - 0
  Backup LSPs UP - 0
  Bypass LSPs - 0
  Bypass LSPs UP - 0
  Bypass LSPs enabled - 0

LDP-Signaled LSPs:
  LSPs operational - 3

Number of times MPLS has been enabled: 1
Next available RSVP LSP tunnel-interface index: 7

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to include the next available RSVP LSP tunnel-interface index.</td>
</tr>
</tbody>
</table>
**show mpls ted database**

Displays the contents of an LSR TED.

**Syntax**

```
show mpls ted database [ node_id detail | detail node_id ]
```

**Parameters**

- `node_id detail`  
  Displays the detailed node identification information.

- `detail node_id`  
  Displays the detailed information of the Traffic Engineering Database (TED) content specified by the `node_id` variable.

**Modes**

User EXEC mode.

**Command Output**

The `show mpls ted database` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AreaID</td>
<td>The identification of this OSPF area.</td>
</tr>
<tr>
<td>NodeID</td>
<td>The identification of the node. For router nodes, can be any interface address or a loopback interface address on the LER. For network nodes, this is the router identification of the network’s designated router.</td>
</tr>
</tbody>
</table>
| (node) Type  | The node type can be either ‘Router’ or ‘Network’.  
  - ‘Router’ indicates the node is an actual LSR.  
  - ‘Network’ indicates the node represents a multi-access network. |
| (link) Type  | The link type can be either ‘P2P’ or ‘M/A’.  
  - ‘P2P’ indicates this is a point-to-point link.  
  - ‘M/A’ indicates the link is a broadcast, multi-access network. |
| To           | The identification of the node at the end of the link. |
| Local        | The address of the interface used to reach the remote node. |
| Remote       | The address of the interface on the remote node that connects to the local node. For M/A types, this is always 0.0.0.0. |
Examples

The following example displays the output of the `show mpls ted database` command.

device# show mpls ted database
AreaID: 0
  NodeID: 2.2.2.2, Type: Router
    Type: M/A, To: 10.1.1.2, Remote: 0.0.0.0
  NodeID: 3.3.3.3, type: Router
    Type: P2P, To: 10.1.1.2, Local: 10.1.1.1, Remote: 10.1.1.2
    Type: M/A, To: 10.1.1.3, Local: 10.1.1.3, Remote: 0.0.0.0
    Type: M/A, To: 10.1.1.2, Local: 10.1.1.1, Remote: 0.0.0.0
  NodeID: 10.1.1.3, Type: Network
    Type: M/A, To: 10.1.1.1, Local: 0.0.0.0, Remote: 0.0.0.0
    Type: M/A, To: 10.6.6.6, Local: 0.0.0.0, Remote: 0.0.0.0
  NodeID: 30.1.1.2, type: Network
    Type: M/A, To: 10.1.1.1, Local: 0.0.0.0, Remote: 0.0.0.0
    Type: M/A, To: 10.2.2.2, Local: 0.0.0.0, Remote: 0.0.0.0
    Type: M/A, To: 10.3.3.3, Local: 0.0.0.0, Remote: 0.0.0.0
show mpls ted path

Displays a traffic path to an IPv4 destination address using a specified set of resource parameters.

Syntax

```
show mpls ted path { ip_addr } [ bandwidth kbps ] [ cspf-comp-mode { use-igp-metric | use-te-metric } ] [ exclude-any name ] [ hop-limit max_hops ] [ include-all name ] [ include-any name ] [ path-name name ] [ priority setup ] [ tie-breaking { least-fill | most-fill | random } ]
```

Parameters

- **ip_addr**
  - The IPv4 address of the destination host.

- **bandwidth**
  - The minimum bandwidth of the path to its destination.

  - **kbps**
    - Enter the bandwidth value in decimal form for kilobits per second units. The valid range is between 0 - 2147483647. When the value entered is larger than 2147483647, then the value is truncated to the max limit of 2147483647 and accepted as the bandwidth input.

- **cspf-comp-mode**
  - Selects CSPF computation mode to use to calculate the path.
    - **use-igp-metric**
      - Selects igp-metric to calculate the path.
    - **use-te-metric**
      - Selects te-metric to calculate the path.

- **exclude-any**
  - Excludes any of the administrative groups.

  - **name**
    - Selects the list of administrative groups to exclude. A list of any combination of administrative groups names or numbers. The valid range for the administrative group number is between 0 - 31. The administrative group name must start with an alphabet character. When entering an invalid range for an administrative group number or name, the CLI prompts a warning message, and then the CLI prompts a warning message. It accepts the CLI but ignores the out of range value.

- **hop-limit**
  - The maximum number of hops for the path to reach its destination.

  - **max-hops**
    - The valid range is between 0 - 255. When an invalid range is entered, an error message displays. When a path to the destination is available, but the hop count for the path is greater than the **max-hops** value, then MPLS indicates that the path is not available.

- **include-all**
  - Includes all of the administrative groups.
name

Selects the list of administrative groups. A list of any combination of administrative groups names or numbers. The valid range for the administrative group number is between 0 - 31. The administrative group name must start with an alphabet character. When an invalid range is entered for an administrative group number or name, then the CLI prompts a warning message, the CLI prompts a warning message. The CLI is accepted, but the out of range value is ignored.

path

Displays by path name.

name

Name of selected path.

priority

The setup priority of the path.

setup

The valid range is between 0 - 7. The default is 7, the lowest setup priority value. When an invalid range is entered, an error message displays. The priority parameter must be entered along with the bandwidth parameter because while setting up an LSP, the setup priority value decides the ability to reserve a bandwidth amount.

tie-breaking

Use when multiple equal-cost paths to a destination exist. The tie-breaking rule selects only one path to display from among multiple equal cost paths. The default is random.

least-fill

Path is selected on least-fill criteria.

most-fill

Path is selected on most-fill criteria.

random

Path is selected randomly.

Modes

User EXEC mode

Usage Guidelines

Command Output

The `show mpls ted path` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path to x.x.x.x found</td>
<td>The IPv4 address of the destination host is found.</td>
</tr>
<tr>
<td>Time taken to compute</td>
<td>The total time taken by CSPF (in milliseconds) to compute this path.</td>
</tr>
<tr>
<td>Hop-count</td>
<td>The hop count of this path.</td>
</tr>
<tr>
<td>Cost</td>
<td>The total cost of this path.</td>
</tr>
</tbody>
</table>
### Output field Description

<table>
<thead>
<tr>
<th>IS-IS</th>
<th>The IS-IS or OSPF or CSPF area ID through which this path traverses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop</td>
<td>The ingress interface IPv4 address at each hop.</td>
</tr>
<tr>
<td>Rtr</td>
<td>The traffic engineering router ID (IPv4 address) at each hop.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the `show mpls ted path` command.

```
device# show mpls ted path 10.12.12.12. hop-limit 2
Path to 10.12.12.12. found! Time taken to compute: 0 msec
Hop-count: 2 Cost: 2000 ISIS Level-1
  Hop 1: 10.1.0.1, Rtr 10.13.13.13
  Hop 2: 10.1.0.2, Rtr 10.12.12.12
```

The following example displays the `show mpls ted path` command for a router where the `exclude-any` parameter is used.

```
device# show mpls ted path 10.11.11.11 exclude-any 0
Path to 10.12.12.12. found! Time taken to compute: 0 msec
Hop-count: 1 Cost: 10 ISIS Level-2
  Hop 1: 10.0.0.13, Rtr 10.11.11.11
```

The following example displays the `show mpls ted path` command using the `hop-limit` parameter when entering an out-of-range parameter value.

```
device# show mpls ted path 10.2.2.2 hop-limit 300
Error- Hop count value is out of range [0-255]
```

When entering an out-of-range parameter value, the following error message displays for the priority parameter:

```
Priority
```
show mpls vll

Displays detailed information about the configurations of the Virtual Leased Lines (VLLs) on the device.

Syntax

```
show mpls vll [ vll_id | vll_name ] [ detail ] [ redundancy ]
show mpls vll brief [ redundancy ]
```

Parameters

- **vll_id**: Displays the selected VLL by ID.
- **vll_name**: Displays the selected named VLL by name.
- **detail**: Displays detailed information of the named VLL.
- **redundancy**: Displays MCT VLLs and VLLs having redundant peers.
- **brief**: Displays brief information of the named VLL.

Modes

- User EXEC mode

Usage Guidelines

The `show mpls vll detail` command displays information about the operational state of the VPLS instance regarding the local endpoints.

Command Output

The `show mpls vll detail` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-point</td>
<td>How packets forward once they reach the egress LER. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>∙ &quot;untagged portnum&quot; - Forward the packet out the specified port as untagged.</td>
</tr>
<tr>
<td></td>
<td>∙ &quot;tagged vlan vlan_id / portnum&quot; - Tag the packet with the specified VLAN ID and forward the packet out the specified port.</td>
</tr>
<tr>
<td></td>
<td>∙ &quot;tagged vlan vlan_id inner-vlan vlan_id&quot; - Tag the packet with the specified outer and inner vlan IDs and forward the packet out the specified port.</td>
</tr>
<tr>
<td></td>
<td>∙ &quot;undefined&quot; - An endpoint has not been configured for this VLL.</td>
</tr>
<tr>
<td>End-point state</td>
<td>The current state of the VLL. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>∙ &quot;UP&quot; VLL is operational - packets can flow.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>“DOWN - configuration incomplete”</td>
<td>A required configuration statement is missing.</td>
</tr>
<tr>
<td>“DOWN - endpoint port to CE is down”</td>
<td>The physical endpoint port that must connect to the Customer Edge device is down, due to a link outage or it is administratively disabled.</td>
</tr>
<tr>
<td>“DOWN - no tunnel LSP to vll-peer”</td>
<td>Cannot find a working LSP.</td>
</tr>
<tr>
<td>“DOWN - PW is Down (Reason: LDP session is down)”</td>
<td>LDP session is not yet ready.</td>
</tr>
<tr>
<td>“DOWN - Waiting for PW Up”</td>
<td>VLL is waiting for MPLS to bring up the session.</td>
</tr>
<tr>
<td>“DOWN - Waiting for VC withdrawal Completion”</td>
<td>PW is down, and VLL is waiting for MPLS to withdraw the labels that VLL has requested.</td>
</tr>
<tr>
<td>“DOWN - PW is Down (Reason: Out of VC labels)”</td>
<td>PW is down; VC labels are not available.</td>
</tr>
<tr>
<td>“DOWN - PW is Down (Reason: Out of Memory)”</td>
<td>PW is down; there is not sufficient memory available.</td>
</tr>
<tr>
<td>“DOWN - PW is Down (Reason: Waiting for Remote VC label)”</td>
<td>PW is down; waiting for remote peer’s VC label to advertise.</td>
</tr>
<tr>
<td>“DOWN - waiting for VC label binding from vll-peer”</td>
<td>The device has advertised its VC label binding to the VLL peer but has not yet received the peer’s VC label binding.</td>
</tr>
<tr>
<td>“DOWN - PW is Down (Reason: MTU mismatch Local- MTU mtu-value, Remote- MTU mtu-value)”</td>
<td>PW is down, and the MTU values for the local and remote peers are not equal.</td>
</tr>
<tr>
<td>“DOWN - PW is Down (Reason: VC type mismatch, Local VC type: vc-type, Remote VC type: vc-type)”</td>
<td>The session cannot be come up because the VC types of the local and remote peers are not equal. The possible value for the vc-type variable is five (5) for raw mode or four (4) for tagged mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MCT state</th>
<th>Options: Active, Passive, NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFL-ID</td>
<td>The Internal Forwarding Lookup Identifier (IFL-ID) allocation to each Local VLL instance that has, at least, one dual-tagged endpoint. For instances that do not have dual-tagged endpoints, the IFL-ID is displayed as “--”.</td>
</tr>
<tr>
<td>Local VC type</td>
<td>Indicates whether the local VC is in raw-mode or tagged-mode.</td>
</tr>
<tr>
<td>Local VC MTU</td>
<td>The MTU value configured for this local VC.</td>
</tr>
<tr>
<td>COS</td>
<td>The optional CoS setting for the VLL. When a CoS value sets, the device attempts to select a tunnel LSP that also has this CoS value. The CoS value can be from 0 through 7.</td>
</tr>
<tr>
<td>Extended Counters</td>
<td>Indicates whether or not the extended counters are enabled for the configured VLL.</td>
</tr>
<tr>
<td>Vll-Peer</td>
<td>The remote PE router. It must be the same as the LSP destination for the LSPs that the VLL transports over.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the VLL. It can be either UP or DOWN. Data can be forwarded over the VLL only when the state is UP.</td>
</tr>
<tr>
<td>Remote VC type</td>
<td>Indicates whether the remote VC is in raw mode or tagged mode.</td>
</tr>
<tr>
<td>Remote VC MTU</td>
<td>The MTU value advertised from the VLL peer.</td>
</tr>
<tr>
<td>Local label</td>
<td>The VC label value locally allocated for this VLL. Packets forwarded from the VLL peer to this device are expected to contain this label. It is the label that is advertised to the VLL peer through LDP.</td>
</tr>
<tr>
<td>Remote label</td>
<td>The VC label allocated by the VLL peer and advertised to this device through LDP. The device applies this label to outbound MPLS packets sent to the VLL peer.</td>
</tr>
</tbody>
</table>
### Output field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local group-id</td>
<td>The VLL group ID (defined in draft-martini-l2circuit-trans-mpls-07.txt) advertised to the VLL peer through LDP. The group ID is always zero.</td>
</tr>
<tr>
<td>Remote group-id</td>
<td>The VLL group ID selected and advertised by the VLL peer.</td>
</tr>
<tr>
<td>Tunnel LSP</td>
<td>The name, as well as the internal tunnel index number, of the tunnel LSP selected for the VLL.</td>
</tr>
</tbody>
</table>
| MCT Status TLV | Options:  
  - Active - Node will start peering with the remote peers, signaling Status TLV as Active.  
  - Standby - Node will start peering with remote peers, signaling Status TLV as Standby.  
  - Transit - MCT VLL is not in the operational state. Remote peering is not yet enabled. |
| LSPs assigned  | Lists the assigned LSPs. |

### Examples

The following example displays the detailed information about the VLL.

```
device# show mpls vll detail

VLL VLL_to_R3, VC-ID 40000, VLL-INDEX 1

  End-point        : untagged e 1/7
  End-Point state  : Up
  MCT state        : None
  IFL-ID           : --
  Local VC type    : tag
  Local VC MTU     : 1500
  COS              : --
  Extended Counters: Enabled

  Vll-Peer         : 192.168.2.102
  State           : UP
  Remote VC type  : tag
  Remote VC MTU   : 1500
  Local label     : 851968
  Remote label    : 851968
  Local group-id  : 0
  Remote group-id : 0
  load balance    : enable
  number of tunnels : 8
  Tunnel LSP      : tnl0[Rsvp],tnl1[Rsvp],tnl2[Rsvp],tnl3[Rsvp],tnl4[Rsvp],tnl5[Rsvp],tnl6[Rsvp],tnl7[Rsvp]
  MCT Status TLV  : --
  LSPs assigned   : No LSPs assigned
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.0</td>
<td>A new addition in the detail option was added to allow the user to select raw pass-through mode. The option behaves like tagged mode when the endpoint is configured as a tagged endpoint or raw mode when the endpoint is configured as an untagged endpoint.</td>
</tr>
<tr>
<td>5.7.0</td>
<td>This command was modified to include the &quot;LSP assigned&quot; field in the display output for show mpls vll detail, show mpls vll vll_name, and show mpls vll vll_id.</td>
</tr>
<tr>
<td>6.0.0</td>
<td>This command was modified to show whether load balancing is enabled, and the number of tunnels.</td>
</tr>
</tbody>
</table>
show mpls vll-local
Displays information about individual Local VLLs configured on the router.

Syntax

```
show mpls vll-local local_vll_name [ brief | detail ]
```

Parameters

- `local_vll_name` Specifies the local VLL name.
- `brief` Displays brief information.
- `detail` Displays detailed information for all local VLLs in the router. Specifying a particular VLL using the `vll-name` option limits the display to the specified Local VLL.

Modes

User EXEC mode.

Command Output

The `show mpls vll-local` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The configured name of the Local VLL.</td>
</tr>
<tr>
<td>VLL-ID</td>
<td>The VLL ID.</td>
</tr>
<tr>
<td>End-point</td>
<td>How packets forward out of the egress port of the Local VLL. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <code>untagged portnum</code> - Forward the packet out the specified port as untagged.</td>
</tr>
<tr>
<td></td>
<td>- <code>tag vlan vlan_id/portnum</code> - Tag the packet with the specified VLAN ID and forward the packet out the specified port.</td>
</tr>
<tr>
<td></td>
<td>- <code>undefined</code> - An endpoint has not been configured for this Local VLL.</td>
</tr>
<tr>
<td></td>
<td>- <code>inner-vlan</code> - describes the inner-vlan tag for an end-point that is configured for dual-tagging.</td>
</tr>
<tr>
<td>IFL-ID</td>
<td>The Internal Forwarding Lookup Identifier (IFL-ID) allocated to each Local VLL instance that has at least one dual tag endpoint. For instances that do not have dual tag endpoints, the IFL-ID is displayed as <code>-</code>.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the Local VLL. It can be one of the following:</td>
</tr>
</tbody>
</table>

Show Commands

NetIron Command Line Interface (CLI) Reference Guide
53-1004199-02 877
### Show Commands

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
<th>Command level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>∙ ‘UP’ - The local VLL is operational - packets can flow.</td>
<td>show mpls vll-local</td>
</tr>
<tr>
<td></td>
<td>∙ ‘DOWN - configuration complete’ - A required configuration statement is missing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>∙ ‘DOWN - endpoint port is down’ - The physical endpoint port is down due to a link outage or is administratively disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>COS</strong></td>
<td>The optional CoS setting for the Local VLL. When a CoS value sets, the CoS value can be between 0 - 7.</td>
<td></td>
</tr>
<tr>
<td><strong>Extended Counters</strong></td>
<td>Indicates whether or not the extended counters are enabled for the configured Local VLL instances.</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example shows the output of the `show mpls vll-local` command:

```device# show mpls vll-local
Name      VLL-ID  End-point1         End-point2         State
foundrylong 1  tag vlan 100 e5/12  undefined          DOWN
villocalfou  ndrylonfvi1 localfoundr vilongvillloc alfoundry test 2  tag vlan 200 inner-vlan 50 e2/1  tag vlan 200 e2/2  UP
```

The following example shows detailed information for all Local VLLs in the router. Using the `vll_name` option limits the display to the specified Local VLL.

```device# show mpls vll-local detail
VLL-test-1 VLL-ID1 IFL-ID- State:UP
End-point1:untagged e2/2  COS:-
End-point2:untagged e2/13  COS:-  Extended Counters:Enabled
VLL-test-2 VLL-ID2 IFL-ID- State:UP
End-point1:tagged vlan 2500 e2/10  COS:-
End-point2:tagged vlan 2500 e2/9  COS:-  Extended Counters:Enabled
VLL-test-3 VLL-ID3 IFL-ID- State:UP
End-point1:tagged vlan 2501 e2/10  COS:6
End-point2:tagged vlan 2501 e2/9  COS:5  Extended Counters:Enabled
VLL-test-4 VLL-ID4 IFL-ID4096 state:UP
End-point1:tagged vlan 100 inner-vlan 45 e2/1  COS:-
End-point2:tagged vlan 100 e2/3  COS:-  Extended Counters:Enabled
```
**show mpls vpls**

Displays information about the VPLS configuration.

**Syntax**

```
show mpls vpls [ brief [ redundancy ] | detail | down | id vpls_id | local | name vpls_name | summary ]
```

**Parameters**

- **brief**
  
  Displays brief information for each VPLS (default).

- **redundancy**
  
  Displays cluster-peer pw redundancy.

- **detail**
  
  Displays detailed information for each VPLS.

- **down**
  
  Displays brief information for each VPLS that is not completely operational.

- **id vpls_id**
  
  Displays detailed information for the VPLS specified by its ID.

- **local**
  
  Displays detailed information for local entry.

- **name vpls_name**
  
  Displays detailed information for the VPLS specified by its name.

- **summary**
  
  Displays summary information.

**Modes**

User EXEC mode

**Usage Guidelines**

When both the VC type and MTU are mismatched, only the output from the VC type mismatch is displayed on the console.

This command operates in all modes.

**Command Output**

**show mpls vpls detail**

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPLS</td>
<td>The configured name of the VPLS instance.</td>
</tr>
<tr>
<td>Max mac entries</td>
<td>The maximum number of MAC entries that can be learned for the VPLS instance.</td>
</tr>
<tr>
<td>Output field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total vlans</td>
<td>The number of VLANs that are translated for this VPLS instance.</td>
</tr>
<tr>
<td>Tagged ports</td>
<td>The total number of tagged ports that are associated with VLANs in this VPLS instance, as well as the number of these ports that are up.</td>
</tr>
<tr>
<td>Untagged ports</td>
<td>The total number of untagged ports that are associated with VLANs in this VPLS instance, as well as the number of these ports that are up.</td>
</tr>
<tr>
<td>IFL-ID</td>
<td>The Internal Forwarding Lookup Identifier (IFL-ID) for dual-tagged ports in the VPLS instance.</td>
</tr>
<tr>
<td>L2 Protocol</td>
<td>Layer 2 control protocol configured on the VLAN.</td>
</tr>
<tr>
<td>Tagged</td>
<td>The numbers of the tagged ports in each VLAN.</td>
</tr>
<tr>
<td>VC-Mode</td>
<td>The VC mode for the VPLS instance.</td>
</tr>
<tr>
<td></td>
<td>- Raw - The VLAN tag information in the original payload is not carried across the MPLS cloud.</td>
</tr>
<tr>
<td></td>
<td>- Tagged - The VLAN tag information in the original payload is carried across the MPLS cloud.</td>
</tr>
<tr>
<td></td>
<td>- Raw pass-through - The VLAN tag information behaves like tagged mode when all endpoints are configured as tagged endpoints.</td>
</tr>
<tr>
<td>Total VPLS peers</td>
<td>The number of VPLS peers this device has for this VPLS instance, as well as the number of these VPLS peers with which this device has an LDP session.</td>
</tr>
<tr>
<td>Peer address</td>
<td>The IP address of the VPLS peer.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the connection with the VPLS peer. This can be one of the following states:</td>
</tr>
<tr>
<td></td>
<td>- Operational - The VPLS instance is operational. Packets can flow between the device and the peer.</td>
</tr>
<tr>
<td></td>
<td>- Wait for functional local ports - The physical endpoint port that must be connected to the Customer Edge device is down due to a link outage or is administratively disabled.</td>
</tr>
<tr>
<td></td>
<td>- Wait for LSP tunnel to Peer - The device cannot find a working tunnel LSP.</td>
</tr>
<tr>
<td></td>
<td>- Wait or PW Up (Wait for LDP session to Peer) - The LDP session is not ready.</td>
</tr>
<tr>
<td></td>
<td>- Wait for PW Up (Wait for remote VC label) - The device has advertised its VC label binding to the VPLS peer, but has not yet received the peer’s VC labeling binding.</td>
</tr>
<tr>
<td></td>
<td>- Wait for PW Up (VC type mismatched) - A session is not formed because the VC type does not match with its peer’s VC type.</td>
</tr>
<tr>
<td></td>
<td>- Wait for PW Up (MTU mismatched) - The MTU sent to a peer is derived from the device’s global setting by the following formula: (system-mtu minus 26 bytes). When a system-mtu value is not configured, a default value of 1500 is sent.</td>
</tr>
<tr>
<td></td>
<td>- Wait for PW Up (Wait for LDP session to Peer) - The LDP session to the peer is down.</td>
</tr>
<tr>
<td></td>
<td>- Wait for PW Up (No label resource) - When configuring a VPLS peer, the maximum number of VC labels that can be supported may exceed 65536 and cause the configuration to be rejected. The maximum number of VC labels available for VPLS instances is equal to 65536.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The time, in minutes, that the entry has been operational.</td>
</tr>
<tr>
<td>Tunnels in use (load balance)</td>
<td>The tunnel LSP used to reach the VPLS peer. When VPLS traffic to the peer is load balanced across multiple tunnel LSPs, the tunnel LSPs used to reach the peer are displayed.</td>
</tr>
<tr>
<td>Local VC lbl</td>
<td>The VC label value locally allocated for this peer for this VPLS instance. Packets forwarded from the VPLS peer to this device are expected to contain this label. This is the label that is advertised to the VPLS peer through LDP.</td>
</tr>
<tr>
<td>Remote VC lbl</td>
<td>The VC label allocated by the VPLS peer and advertised to this device through LDP. The device applies this label to outbound MPLS packets sent to the VPLS peer.</td>
</tr>
<tr>
<td>Local VC MTU</td>
<td>The MTU value locally configured for this peer.</td>
</tr>
</tbody>
</table>
### Output field
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote VC MTU</td>
</tr>
<tr>
<td>Local VC-Type</td>
</tr>
<tr>
<td>Remote VC-Type</td>
</tr>
<tr>
<td>CPU-Protection</td>
</tr>
<tr>
<td>Local Switching</td>
</tr>
<tr>
<td>Extended Counter</td>
</tr>
<tr>
<td>Multicast Snooping</td>
</tr>
</tbody>
</table>

### Examples
The following example displays the output of the `show mpls vpls brief redundancy` command.

```
device# show mpls vpls brief redundancy

Name  Id  Up  Peers  MCT  PW-Role  State
-----  --  ----  ------  ------  --------  -----
tst   10  2    2      2      Active  OPER
```

---

**Show Commands**

**Netiron Command Line Interface (CLI) Reference Guide**

53-1004199-02 881
The following example displays the output of the `show mpls vpls detail` command.

```
device# show mpls vpls detail
VPLS 1001, Id 1001, Max mac entries: 32000
Total vlans: 2, Tagged ports: 1 (1 Up), Untagged ports 0 (0 Up)
IFL-ID: 4096
Vlan 1001
  Tagged: ethe 14/3
Vlan 1001 inner-vlan 1001
  Tagged: ethe 14/3
VC-Mode: Raw
Total VPLS peers: 6 (6 Operational)
Peer address: 10.0.0.1, State: Operational, Uptime: 1 hr 44 min
  LSPs assigned: f1a1 a1a2 a2a5 a3a8, Tnnls in use (load balance): Candidate count:1 (only 1st 4 is displayed):
    tnl0(1217)[RSVP]  Peer Index:0
    Local VC lbl: 983839, Remote VC lbl: 984238
    Local VC MTU: 9190, Remote VC MTU: 9190
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
    Peer address: 10.0.0.2, State: Operational, Uptime: 1 hr 44 min
  LSPs assigned: f1b1 a1b2 a2b5 a3b8, Tnnls in use (load balance): Candidate count:1 (only 1st 4 is displayed):
    tnl4(1075)[RSVP]  Peer Index:1
    Local VC lbl: 983239, Remote VC lbl: 984238
    Local VC MTU: 9190, Remote VC MTU: 9190
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
    Peer address: 10.0.0.3, State: Operational, Uptime: 1 hr 37 min
  LSPs assigned: f1c1 a1c2 a2c5 a3c8, Tnnls in use (load balance): Candidate count:1 (only 1st 4 is displayed):
    tnl8(1193)[RSVP]  Peer Index:2
    Local VC lbl: 983439, Remote VC lbl: 983240
    Local VC MTU: 9190, Remote VC MTU: 9190
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
    Peer address: 10.0.0.4, State: Operational, Uptime: 1 hr 44 min
  LSPs assigned: f1d1 a1d2 a2d5 a3d8, Tnnls in use (load balance): Candidate count:1 (only 1st 4 is displayed):
    tnl12(1355)[RSVP] Peer Index:3
    Local VC lbl: 983639, Remote VC lbl: 984039
    Local VC MTU: 9190, Remote VC MTU: 9190
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
    Peer address: 10.0.0.5, State: Operational, Uptime: 1 hr 37 min
  LSPs assigned: f1e1 a1e2 a2e5 a3e8, Tnnls in use (load balance): Candidate count:1 (only 1st 4 is displayed):
    tnl16(1071)[RSVP] Peer Index:4
    Local VC lbl: 983839, Remote VC lbl: 984238
    Local VC MTU: 9190, Remote VC MTU: 9190
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
    Peer address: 10.0.0.6, State: Operational, Uptime: 1 hr 37 min
  LSPs assigned: f1g1 a1g2 a2g5 a3g8, Tnnls in use (load balance): Candidate count:1 (only 1st 4 is displayed):
    tnl20(1374)[RSVP] Peer Index:5
    Local VC lbl: 984439, Remote VC lbl: 983840
    Local VC MTU: 9190, Remote VC MTU: 9190
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
CPU-Protection: OFF
Local Switching: Enabled
Extended Counter: ON
Multicast Snooping: Disabled
```
The following example shows when the remote peer is in an operational state. The total VC labels allocated field no longer displays in the output of the `show mpls vpls id vpls_id` command.

device# show mpls vpls id 3
VPLS name_raw, Id 3, Max mac entries: 8192
Total vlans: 1, Tagged ports: 3 (3 Up), Untagged ports 0 (0 Up)
  IFL-ID: 4097
  Vlan 300 inner-vlan 500
  Tagged: ethe 3/1 ethe 3/11 ethe 3/13
VC-Mode: Raw
Total VPLS peers: 1 (1 Operational)
Peer address: 10.200.200.200, State: Operational
  Uptime: 1 hr 10 min
  Tnln in use: tnln(4)
    LDP session: Up, Local VC lbl: 983072, Remote VC lbl: 983072
    Local VC MTU: 1500, Remote VC MTU: 1500
    LOCAL VC-Type: Ethernet (0x05), Remote VC-Type: Ethernet (0x05)
CPU-Protection: OFF
Local Switching: Enable

The following example shows the MCT support for VE over VPLS.

device# show mpls vpls id 3
VPLS vevpls, Id 100, Max mac entries: 2048
Routing Interface Id 100
Total vlans: 1, Tagged ports: 1 (1 Up), Untagged ports 0 (0 Up)
  IFL-ID: n/a
  Vlan 100
    L2 Protocol: NONE
    Tagged: ethe 1/20
VC-Mode: Raw
Total VPLS peers: 2 (2 Operational)
  Tnln in use: tnln(2049) [RSVP] Peer Index:0
    Local VC lbl: 983042, Remote VC lbl: 983040
    Local VC MTU: 1500, Remote VC MTU: 1500
    LOCAL VC-Type: Ethernet (0x05), Remote VC-Type: Ethernet (0x05)
Peer address: 9.9.9.9, State: Operational, Uptime: 3 min
  Tnln in use: tnln(3) [RSVP] Peer Index:1
    Local VC lbl: 983041, Remote VC lbl: 983040
    Local VC MTU: 1500, Remote VC MTU: 1500
    Local PW preferential Status:Active, Remote PW preferential Status:Active
    Local VC-Type: Ethernet (0x05), Remote VC-Type: Ethernet (0x05)
CPU-Protection: OFF
Local Switching: Enabled
Extended Counter: ON
Multicast Snooping: Disabled
Cluster-peer: enabled, Role:Active State: VPLS_MCT_STATE опер
Vrrp-MCT-aware: enabled

The following example displays the output of the `show mpls vpls name vpls_name` command.

device# show mpls vpls name c1
VPLS cl1, Id 10, Max mac entries: 8192
Total vlans: 0, Tagged ports: 0 (0 Up), Untagged ports 0 (0 Up)
Total VPLS peers: 1 (0 Operational)
auto-discovery enabled, RD 10:10
export RT 10:10
import RT 10:10
Peer address: 10.2.2.2 (auto-discovered)
  State: Wait for functional local ports
  Tnln in use: (load balance)
  : None
    LDP session: Up, Local VC lbl: 983040, Remote VC lbl: N/A
    Local VC MTU: 1500, Remote VC MTU: 0
CPU-Protection: OFF
Local Switching: Enabled
The following example displays the output of the `show mpls vpls summary` command.

device# show mpls vpls summary
Virtual Private LAN Service summary:
  Total VPLS configured: 4072, maximum number of VPLS allowed: 4096
  Total number of IFL-ID's allocated by VPLS: 0
  Total VPLS peers configured: 8139, total peers operational: 8138
  Total VPLS Local end-points configured: 0
  Maximum VPLS mac entries allowed: 160000, currently installed: 150530
  VPLS global raw mode VC-Type is Ethernet (0x05)
  VPLS global MTU is 8974, MTU enforcement is OFF
  Global CPU protection: OFF
  VPLS policy parameters:
    vpls-pw-redundancy: 1
    MVIDs in use: 0 of 1 total allocated
    mac-address withdrawal-limit: 500
    MAC age time for local: 300
    MAC age time for remote: 600

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command output was modified to display VPLS instance ID if RSTP is running on a VPLS VLAN. The total VC labels allocated field is no longer displayed in the output of the <code>show mpls vpls name vpls_name</code> command.</td>
</tr>
<tr>
<td>5.5.00</td>
<td>This command was modified to include the <code>raw pass-through</code> option for the VC-Mode field. The MAC age time for local and MAC age time for remote fields were added.</td>
</tr>
<tr>
<td>5.6.00</td>
<td>VPLS Manual LSP assignment for a peer can now accept a maximum of eight LSPs instead of four LSPs.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>The <code>show mpls vpls summary</code> command output was modified to include information about the total configured VPLS local endpoints in the system.</td>
</tr>
</tbody>
</table>
show mstp
Displays Multiple Spanning Tree Protocol (MSTP) information.

Syntax
show mstp [ blocked [ mstp-id | region region_id ] | mstp-id [ region region_id ] ]

Parameters
blocked
Specifies the display information in respect of ports blocked by the MSTP only.
mstp-id
Specifies the display of information for a specific MSTP instance.
region region-id
Specifies the display of information for a specific MSTP region.
builted
Specifies the display information in respect of ports blocked by the MSTP only.

Modes
User EXEC mode

Usage Guidelines
This command can also be entered in global configuration mode.

History
<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>The command was modified to display only ports blocked by the Multiple Spanning Tree Protocol.</td>
</tr>
</tbody>
</table>
show mvrp
Displays Multiple VLAN Registration Protocol (MVRP) information.

Syntax
`show mvrp [ ethernet slot/port ]`

Parameters
- `ethernet slot port`
  Displays MVRP information for a specific Ethernet port.

Modes
- User EXEC mode

Usage Guidelines
MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Examples
The following example displays MVRP information for all interfaces.
```
device> show mvrp
---------------------------------------------------------
Total configured mvrp ports : 2
Global Status : Enabled
Join-timer(in ms) : 200
Leave-timer(in ms) : 1000
Leaveall-timer(in ms) : 10000
---------------------------------------------------------
MVRP Port(s): ethe 1/1 to 1/5, ethe 1/7, ethe 1/9 to 1/11
```
The following example displays MVRP information for Ethernet interface 1/1.
```
device> show mvrp ethernet 1/1
-----------------------------------------------------------
MVRP Status : Enabled
Join-timer(in ms) : 200
Leave-timer(in ms) : 1000
Leaveall-timer(in ms) : 10000
P2p : No
Applicant Mode : normal-participant
-----------------------------------------------------------
Registered Vlan(s) : 1 to 60 77 100 to 500 999
Declared Vlan(s) : 1 to 60 77 100 to 500 999
Forbidden Vlan(s) : 10
-----------------------------------------------------------
```
show mvrp attributes
Displays Multiple VLAN Registration Protocol (MVRP) attribute information.

Syntax
```
show mvrp attributes [ ethernet slot/port ] [ vlan vlan-id ]
```

Parameters
- **ethernet slot port**
  Displays MVRP attribute information for a specific Ethernet port.
- **vlan vlan-id**
  Displays MVRP attribute information for a specific virtual LAN (VLAN).

Modes
User EXEC mode

Usage Guidelines
MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Use this command to display MVRP attribute information for all ports (and optionally, VLANs) that are registered with MVRP on the network. If no keyword options are used, information about all interfaces and VLANs that are registered as MVRP members is displayed.

Examples
The following example displays MVRP attributes for all ports and VLANs.
```
device> show mvrp attributes

Port : 1/1	State : Forwarding
---------------------------------------------------------------
VLAN  Registrar  Registrar  Applicant
      State     Mgmt     State
---------------------------------------------------------------
  11  IN        FIXED         Very Anxious Observer
  12  IN        FIXED         Very Anxious Observer

Port : 1/2	State : Disabled
---------------------------------------------------------------
VLAN  Registrar  Registrar  Applicant
      State     Mgmt     State
---------------------------------------------------------------
  11  IN        FIXED         Very Anxious Observer
```
The following example displays MVRP attributes for Ethernet interface 1/1.

```
device> show mvrp attributes ethernet 1/1
```

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Blocking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Registrar</th>
<th>Registrar</th>
<th>Applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>State</td>
<td>Mgmt</td>
<td>State</td>
</tr>
<tr>
<td>11</td>
<td>IN</td>
<td>FIXED</td>
<td>Very Anxious Observer</td>
</tr>
<tr>
<td>12</td>
<td>IN</td>
<td>FIXED</td>
<td>Very Anxious Observer</td>
</tr>
</tbody>
</table>

The following example displays MVRP attributes for VLAN 11

```
device> show mvrp attributes vlan 100
```

<table>
<thead>
<tr>
<th>PORT</th>
<th>VLAN</th>
<th>Registrar</th>
<th>Registrar</th>
<th>Applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>State</td>
<td>Mgmt</td>
<td>State</td>
</tr>
<tr>
<td>1/1</td>
<td>11</td>
<td>IN</td>
<td>FIXED</td>
<td>Very Anxious Observer</td>
</tr>
<tr>
<td>1/2</td>
<td>11</td>
<td>IN</td>
<td>FIXED</td>
<td>Very Anxious Observer</td>
</tr>
<tr>
<td>1/3</td>
<td>11</td>
<td>IN</td>
<td>FIXED</td>
<td>Very Anxious Observer</td>
</tr>
</tbody>
</table>
show mvrp config

Displays Multiple VLAN Registration Protocol (MVRP) configuration information.

Syntax

    show mvrp config

Modes

    User EXEC mode

Usage Guidelines

MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Use this command to review the MVRP parameters configured on this device.

Examples

The following example displays the MVRP parameters configured on this device.

device> show mvrp config

    mvrp enable
    mvrp timer join 400 leave 2000 leave-all 10000
    !
    interface ethernet 1/5
    !
    mvrp enable
    mvrp registration-mode forbidden vlan 10
    mvrp timer join 400 leave 1500 leave-all 8000
    mvrp point-to-point
    mvrp applicant-mode non-participant
show mvrp statistics

Displays Multiple VLAN Registration Protocol (MVRP) statistics.

Syntax

```plaintext
show mvrp statistics [ ethernet slot/port ]
```

Parameters

- `ethernet slot port`
  Displays MVRP statistics for a specific Ethernet port.

Modes

- User EXEC mode

Usage Guidelines

MVRP allows the propagation of VLAN information from device to device. With MVRP, an access switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.

Use this command to display MVRP statistics for all ports that are registered with MVRP on the network. If no keyword options are used, statistical information about all interfaces that are registered as MVRP members is displayed.

Examples

The following example displays MVRP statistics for all ports.

device> show mvrp statistics

<table>
<thead>
<tr>
<th>Port</th>
<th>: ethe 1/1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message type</td>
</tr>
<tr>
<td>New</td>
<td></td>
</tr>
<tr>
<td>In</td>
<td></td>
</tr>
<tr>
<td>Join In</td>
<td></td>
</tr>
<tr>
<td>Join Empty</td>
<td></td>
</tr>
<tr>
<td>Empty</td>
<td></td>
</tr>
<tr>
<td>Leave</td>
<td></td>
</tr>
<tr>
<td>Leave-all</td>
<td></td>
</tr>
<tr>
<td>Total PDUs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>: ethe 1/2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message type</td>
</tr>
<tr>
<td>New</td>
<td></td>
</tr>
<tr>
<td>In</td>
<td></td>
</tr>
<tr>
<td>Join In</td>
<td></td>
</tr>
<tr>
<td>Join Empty</td>
<td></td>
</tr>
<tr>
<td>Empty</td>
<td></td>
</tr>
<tr>
<td>Leave</td>
<td></td>
</tr>
<tr>
<td>Leave-all</td>
<td></td>
</tr>
<tr>
<td>Total PDUs</td>
<td></td>
</tr>
</tbody>
</table>
The following example displays MVRP statistics for Ethernet interface 1/1.

```
device> show mvrp statistics ethernet 1/1
```

Port : ethe 1/1

<table>
<thead>
<tr>
<th>Message type</th>
<th>Received</th>
<th>Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>In</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Join In</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Join Empty</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Empty</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Leave</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Leave-all</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total PDUs</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show nht-table ipsec-based

Displays the NHT entries created for IPsec processing.

Syntax

show nht-table ipsec-based

Modes

Privileged EXEC mode

Examples

The following example shows the NHT entries created for IPsec processing.

device#show nht-table ipsec-based
Reconcile Done -
   ARP = 0, GRE = 0, MPLS = 0, phase_1 = 0, l2vpn = 0, phase_2 = 0
NHT IP    Index   MAC Address     VLAN    Out I/F  Out Port  TNL CNT XC CNT  LABEL/SPIid     EXP/PCP
1.1.1.2   1       0024.38a5.5130   1        2/1        2/1           1              0             0
device#

device#show nht-table ipsec-based
NHT IP     Index   MAC Address     VLAN  Out I/F  Out Port  LABEL/SPIid  EXP/PCP
1.1.1.2    1      0024.38a5.5130   1      2/1        2/1           0
device#

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show openflow
Displays the configured OpenFlow parameters.

Syntax

```
show openflow
```

Modes

User EXEC mode

Command Output

The `show openflow` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Status</td>
<td>Enable or disable status</td>
</tr>
<tr>
<td>Controller Type</td>
<td>OpenFlow 1.0 or OpenFlow 1.3 controller</td>
</tr>
<tr>
<td>Controller</td>
<td>Number of controllers</td>
</tr>
</tbody>
</table>
Examples

The following example displays the results of the `show openflow` command:

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)
                              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_ESTABLISHED
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_ESTABLISHED
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_ESTABLISHED
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

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.7.00</td>
<td>This command was modified for OpenFlow 1.3</td>
</tr>
</tbody>
</table>
**show openflow controller**

Displays the controller information in a flow.

**Syntax**

```
show openflow controller
```

**Modes**

User EXEC mode

**Command Output**

The `show openflow controller` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Gives the active and passive connection of the controller.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the port</td>
</tr>
<tr>
<td>Port</td>
<td>Port number</td>
</tr>
<tr>
<td>Status</td>
<td>After the connection and OpenFlow handshake, the controller gives the role of OpenFlow channel.</td>
</tr>
<tr>
<td>Role</td>
<td>Equal, Master and Slave role for the controller.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the results of the `show openflow controller` command.

```
device# show openflow controller
------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Contlr Mode</th>
<th>TCP/SSL IP-address</th>
<th>Port</th>
<th>Status</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Equal)</td>
<td>passive TCP 0.0.0.0</td>
<td>6633</td>
<td>TCP_LISTENING</td>
<td></td>
</tr>
<tr>
<td>2 (Master)</td>
<td>active TCP 10.25.128.179</td>
<td>6633</td>
<td>OPENFLOW_ESABLISHED</td>
<td></td>
</tr>
<tr>
<td>3 (Slave)</td>
<td>active TCP 10.25.128.165</td>
<td>6633</td>
<td>OPENFLOW_ESABLISHED</td>
<td></td>
</tr>
</tbody>
</table>
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.7.00</td>
<td>This command was modified to give information about the role of the controller.</td>
</tr>
</tbody>
</table>
show openflow flows

Displays the flows information on the OpenFlow ports.

Syntax

show openflow flows

Modes

User EXEC mode

Command Output

The `show openflow flows` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow</td>
<td>Number of flows</td>
</tr>
<tr>
<td>Packet</td>
<td>Total Number of data packets trapped to be sent to controller</td>
</tr>
<tr>
<td>Byte</td>
<td>Total Number of data bytes trapped to be sent to controller</td>
</tr>
</tbody>
</table>

Examples

The following example displays the output for MP.

```
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
```
The following example displays the output for LP.

device# show openflow flows

Total Number of data packets trapped to be sent to controller: 0
Total Number of data bytes trapped to be sent to controller: 0

Total Number of Flows: 1

Flow Id: 1, Priority: 32768, FD Id: 0, PW Id: 1
Rule:
  In Port: e2/1
  Action: FORWARD
  Out Port: e2/1, Queue: 4

  FID: -N/A-, MVID: -N/A-

Hardware Information:
  Port: 2/1  PPCR Id: 3, CAM Index: 0x000576ac (L4)  PRAM Index: 0x0003ff5e Packets: 0
Statistics:
  Total Pkts: 0
  Total Bytes: 0

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.7.00</td>
<td>This command was modified for OpenFlow 1.3</td>
</tr>
</tbody>
</table>
show openflow groups

For a group or a range of groups, displays the maximum number of actions in a bucket, the maximum number of buckets in a group, and the maximum number of groups.

Syntax

show openflow groups [ group-id ]
show openflow groups group-id to group-id

Parameters

- groups group-id
  Displays details of an OpenFlow group or range of groups.

  to
  Indicates a range of groups.

Modes

User EXEC mode

Command Output

The `show openflow groups` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Maximum number of groups in a flow</td>
</tr>
<tr>
<td>Bucket</td>
<td>Number of buckets per group</td>
</tr>
<tr>
<td>Action</td>
<td>Number of actions per bucket</td>
</tr>
</tbody>
</table>
Examples

The following example displays the output from the `show openflow groups` command.

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      : 64
Max number of buckets in SELECT group: 12
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

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port Number</td>
</tr>
<tr>
<td>Link</td>
<td>Link status</td>
</tr>
<tr>
<td>Speed</td>
<td>Configured speed</td>
</tr>
<tr>
<td>Tag</td>
<td>Tag status</td>
</tr>
<tr>
<td>Mac Address</td>
<td>MAC address of the port</td>
</tr>
<tr>
<td>Mode</td>
<td>Gives the information about the layers</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Link</th>
<th>Speed</th>
<th>Tag</th>
<th>MAC</th>
<th>OF-portid Name</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Up</td>
<td>1G</td>
<td>Yes</td>
<td>000c.dbf5.bd00</td>
<td>1</td>
<td>Layer2</td>
</tr>
<tr>
<td>1/2</td>
<td>Up</td>
<td>1G</td>
<td>Yes</td>
<td>000c.dbf5.bd01</td>
<td>2</td>
<td>Layer2</td>
</tr>
<tr>
<td>1/3</td>
<td>Up</td>
<td>1G</td>
<td>Yes</td>
<td>000c.dbf5.bd01</td>
<td>3</td>
<td>Hybrid-Layer3</td>
</tr>
<tr>
<td>1/4</td>
<td>Up</td>
<td>1G</td>
<td>Yes</td>
<td>000c.dbf5.bd01</td>
<td>4</td>
<td>Hybrid-Layer3</td>
</tr>
<tr>
<td>1/5</td>
<td>Up</td>
<td>1G</td>
<td>Yes</td>
<td>000c.dbf5.bd01</td>
<td>5</td>
<td>Hybrid-Layer3</td>
</tr>
</tbody>
</table>
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show openflow meters
Displays all the meters in a OpenFlow flow.

Syntax

`show openflow meters [ meter-id ]`

Parameters

`meters meter-id`
Shows details of a specific OpenFlow meter.

Modes

User EXEC mode

Command Output

The `show openflow meters` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meter-id</td>
<td>Meter number</td>
</tr>
<tr>
<td>Band</td>
<td>Number of bands in a meter</td>
</tr>
<tr>
<td>Band type</td>
<td>Band type ( supported type: Drop, DSCP_REMARK)</td>
</tr>
<tr>
<td>Rate</td>
<td>Rate of the band</td>
</tr>
<tr>
<td>Counter</td>
<td>Band specific counter</td>
</tr>
</tbody>
</table>
Examples

The following example displays output with specific meter in MP.

```
device(config)# show openflow meters 2
Meter id: 2

Transaction id: 1438
Meter Flags: KBPS BURST STATS
Flow Count: 0
Number of bands: 2
In packet count: -NA-
In byte count: 0

Band Type: DSCP-REMARK
  Rate: 750000
  Burst size: 1500 kb
  Prec level: 1
  In packet band count: -NA-
  In byte band count: 0

Band Type: DROP
  Rate: 1000000
  Burst size: 2000 kb
  In packet band count: -NA-
  In byte band count: 0
```

Total no. of entries printed: 1

The following example displays output with specific meter in LP.

```
device(config)# show openflow meters 1
Meter id: 1023

Meter Flags: KBPS BURST
Number of bands: 2
RL Class Index: 33 33
In packet count: -NA-
In byte count: 0

Band Type: DROP
  Rate: 3000
  Burst size: 1250 kb
  In packet band count: -NA-
  In byte band count: 0

Band Type: DSCP-REMARK
  Rate: 1700
  Burst size: 1250 kb
  Prec level: 27
  In packet band count: -NA-
  In byte band count: 0
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show openflow queues
Displays the queues on the OpenFlow ports.

Syntax

```
show openflow queues [ ethernet slot / port ]
show openflow queues [ ethernet slot / port to slot / port ]
```

Parameters

- `ethernet slot / port`
  Gives information about a particular slot and port in an ethernet.

- `to`
  Indicates a range of ports.

Modes

User EXEC mode

Usage Guidelines

You can specify additional ports with additional `ethernet slot / port` elements.

You can specify additional ports ranges with additional `ethernet slot / port to slot / port` elements.

Command Output

The `show openflow queues` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue</td>
<td>Number of queues</td>
</tr>
<tr>
<td>Rate</td>
<td>Minimum and maximum rate of the queue</td>
</tr>
<tr>
<td>Packet</td>
<td>Number of packet in the queue</td>
</tr>
<tr>
<td>Bytes</td>
<td>Number of bytes in the queue</td>
</tr>
</tbody>
</table>
Examples

The following example displays openflow queues on a specified port.

device#show openflow queues ethernet 2/1

<table>
<thead>
<tr>
<th>Openflow Port</th>
<th>Queue</th>
<th>Min Rate: 0</th>
<th>Max Rate: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>0</td>
<td>Tx Packets: 0</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>1</td>
<td>Tx Bytes: 0</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>2</td>
<td>Tx Packets: 0</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>3</td>
<td>Tx Bytes: 0</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>4</td>
<td>Tx Packets: 1918620</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>5</td>
<td>Tx Bytes: 168838560</td>
<td></td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show pim interface
Displays the IPv4 or IPv6 PIM interface table.

Syntax
show { ip | ipv6 } pim interface

Parameters
ip
Displays the IPv4 PIM interface table.
ipv6
Displays the IPv6 PIM interface table.

Modes
User EXEC mode

Examples
The following is a sample display of the show ip pim interface command.

device# show ip pim interface

---------+--------+---+---+------------+---+---------+-------+----+----+-------+
  Interface|Local   |Ver|St |Router      |TTL|Multicast| Filter|VRF | DR |Override
           |Address |   |   |Address Port|Thr|Boundary | ACL   |    |Prio|Interval
---------+--------+---+---+------------+---+---------+-------+----+----+-------+
e1/3      3.3.3.1 DMv2 Ena Itself       1   None       10   default 1   3000ms
  e1/2      2.2.2.1 DMv2 Ena 2.2.2.2 1/2  1   None       None default 1   3000ms
---------+--------+---+---+------------+---+---------+-------+----+----+-------+
Total Number of Interfaces: 2

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to display neighbor routers on an interface.</td>
</tr>
</tbody>
</table>
show pim multicast-filter

Displays the multicast filters on a interface or globally for the hardware.

Syntax

show { ip | ipv6 } pim

Modes

User EXEC mode

Examples

Show output for global.

device# show ip pim vrf multicast-filter

<table>
<thead>
<tr>
<th>Interface</th>
<th>LAG Member</th>
<th>port</th>
<th>vlan</th>
<th>Multicast Filter</th>
<th>CAM Index</th>
<th>ProgTM</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>-</td>
<td>*</td>
<td>*</td>
<td>1.1.1.1, 239.1.1.1</td>
<td>0x343</td>
<td>22:01:33</td>
</tr>
<tr>
<td>*</td>
<td>-</td>
<td>*</td>
<td>*</td>
<td>*, 234.1.1.1</td>
<td>0x344</td>
<td>22:01:33</td>
</tr>
</tbody>
</table>

Show output for interface .

device# show ip pim interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>LAG Member</th>
<th>port</th>
<th>vlan</th>
<th>Multicast Filter</th>
<th>CAM Index</th>
<th>ProgTM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ve100</td>
<td>-</td>
<td>*</td>
<td>100</td>
<td>1.1.1.1, 239.1.1.1</td>
<td>0x343</td>
<td>22:01:33</td>
</tr>
<tr>
<td>ve102</td>
<td>-</td>
<td>*</td>
<td>100</td>
<td>*, 234.1.1.1</td>
<td>0x344</td>
<td>22:01:33</td>
</tr>
<tr>
<td>e1/13</td>
<td>-</td>
<td>142</td>
<td>100</td>
<td>*, 228/8</td>
<td>0x355</td>
<td>22:01:33</td>
</tr>
<tr>
<td>Tr1(e1/1)</td>
<td>e1/1</td>
<td>155</td>
<td>1</td>
<td>*, 228/8</td>
<td>0x356</td>
<td>22:01:33</td>
</tr>
<tr>
<td>Tn1</td>
<td>-</td>
<td>*</td>
<td>*</td>
<td>*, 228/8</td>
<td>0x358</td>
<td>22:01:33</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>NI0S.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show pki certificates
Displays certificate information associated with a trustpoint or the local router.

Syntax

`show pki certificates trustpoint trustpoint-name [ detail ]`
`show pki certificates local [ detail ]`

Parameters

- `trustpoint trustpoint-name`
  Displays certificate information associated with a trustpoint certificate authority (CA).
- `detail`
  Displays detailed information about the certificate.
- `local`
  Displays certificate information associated with a local certificate provided for the device.
- `detail`
  Displays detailed information about the certificate.

Modes

User EXEC mode

Examples

The following example displays output for the trustpoint with the name “brocade”.

device# show pki certificates trustpoint brocade

----------------PKI TRUSTPOINT CERTIFICATE ENTRY----------------
Certificate:
  Data:
   Version: 3 (0x00000002)
   Signature Algorithm: ecdsa-with-SHA1
   Issuer: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
   emailAddress=brocade_ca@brocade.com
   Validity
     Not Before: Aug 29 05:58:13 2014 GMT
     Not After: Aug 29 05:58:13 2019 GMT
   Subject: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
   emailAddress=brocade_ca@brocade.com
The following example displays the detailed output for the trustpoint with the name "brocade".

device# show pki certificates trustpoint brocade detail

--------------PKI TRUSTPOINT CERTIFICATE ENTRY--------------
Certificate:
  Data:
    Version: 3 (0x00000002)
    Signature Algorithm: ecdsa-with-SHA1
    Issuer: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
            emailAddress=brocade_ca@brocade.com
    Validity
      Not Before: Aug 29 05:58:13 2014 GMT
      Not After : Aug 29 05:58:13 2019 GMT
    Subject: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_CA/
             emailAddress=brocade_ca@brocade.com
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (384 bit)
      pub:
        08:8b:ed:01:14:3d:41:ec:0a:98:85:2a:4b:0e:
        b8:7e:5f:83:01:14:16
      ASN1 OID: secp384r1
    X509v3 extensions:
      X509v3 Subject Key Identifier:
      X509v3 Authority Key Identifier:

      X509v3 Basic Constraints:
      X509 CA:TRUE
      Signature Algorithm: ecdsa-with-SHA1

The following example displays the output for the local certificate.

device# show pki certificates local

--------------PKI LOCAL CERTIFICATE ENTRY--------------
Certificate:
  Data:
    Version: 3 (0x00000002)
    Serial Number: 1 (0x00000001)
    Signature Algorithm: ecdsa-with-SHA1
    Issuer: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_RA/
            emailAddress=brocade_ra@brocade.com
    Validity
      Not Before: Sep 10 14:55:12 2014 GMT
      Not After : Jun  1 14:55:12 2016 GMT
    Subject: C=IN, ST=Karnataka, L=Bangalore, O=Brocade, OU=Routing, CN=Brocade_RA/
             emailAddress=brocade_ra@brocade.com

Netiron Command Line Interface (CLI) Reference Guide
S3-1004199-02
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show pki counters
Displays the Public Key Infrastructure (PKI) counter information for a certificate authority (CA).

Syntax
show pki counters

Modes
User EXEC mode

Examples
The following example displays information about the PKI counter information for a CA.

device# show pki counters
PKI Sessions Started: 5
PKI Sessions Ended: 5
PKI Sessions Active: 0
Successful Validations: 1
Failed Validations: 4
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 3
CRL - fetch attempts: 2
CRL - failed attempts: 0

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show pki crls
Displays the Public Key Infrastructure (PKI) Certification Revocation list (CRL).

Syntax
show pki crls trustpoint name

Parameters
trustpoint name
The specific trustpoint name whose PKI CRLs need to be displayed.

Modes
User EXEC mode

Examples
The following example displays the PKI CRL list.

device# show pki crls
CRL Issuer Name:
   cn=name Cert Manager,ou=pki,o=company.com,c=US
CRL number: 24
CRL Version: V2
LastUpdate: 18:57:42 GMT March 4 2013
NextUpdate: 22:57:42 GMT March 4 2013
Retrieved from CRL Distribution Point:
   via SCEP

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show pki enrollment-profile

Displays the Public Key Infrastructure (PKI) enrollment profile details.

Syntax

```
show pki enrollment-profile profile name
```

Parameters

`profile name`

Specifies the PKI enrollment profile name.

Modes

User EXEC mode

Examples

The following example displays information about the PKI enrollment profiles.

```
device# show pki enrollment-profile

----------------PKI ENROLLMENT PROFILE ENTRY-----------------
Enrollment Profile: John
Authentication Command: win-hj98ak136a0.englab.brocade.com_englab-WIN-N6C3RULUDAJ-CA-7
Authentication URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
Enrollment URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
SCEP password: 8A4976CE110A8686

----------------PKI ENROLLMENT PROFILE ENTRY-----------------
Enrollment Profile: Jane

----------------PKI ENROLLMENT PROFILE ENTRY-----------------
Enrollment Profile: John
Authentication Command: win-hj98ak136a0.englab.brocade.com_englab-WIN-N6C3RULUDAJ-CA-7
Authentication URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
Enrollment URL: http://win-hj98ak136a0.englab.brocade.com/CertSrv/mscep/mscep.dll
SCEP password: 8A4976CE110A8686
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

S3-1004199-02

Page 92
show pki entity

Displays the PKI entity details.

Syntax

show pki entity entity-name

Parameters

entity-name

The entity name.

Modes

User EXEC mode

Examples

The following example displays the output for the entity name "brocade_entity".

device# show pki entity brocade_entity

----------------PKI ENTITY ENTRY-----------------
Entity Name: brocade_entity
Common Name: brocade_e
Organization Name: Brocade
Organization Unit Name: Routing
State Name: Karnataka
Country Name: India
Email: user@brocade.com
FQDN: brocade-fqdn
Subject Alternative Name: brocade-subject
Location: Bangalore
IP Address: 1.1.1.1

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show pki key mypubkey

Displays the PKI public keys on the NetIron device.

**Syntax**

`show pki key mypubkey ec manual [ label label-string ]`

**Parameters**

- **ec**
  The manually configured Elliptic Curve (EC) key.
- **manual**
  The manually configured key.
- **label**
  The ID given to the key.
- **label-string**
  The name of the label.

**Modes**

User EXEC mode

**Examples**

The following example displays the output for the manually generated PKI keys.

```
device# show pki key mypubkey ec manual label xmr-key
```

```
----------------PKI PUBLIC KEY ENTRY----------------
Public key of manual EC key pair:
The key label is xmr-key
Public-Key: (384 bit)
pub:
22:eb:de:27:58:d6:00:66:f0:cc:7f:d2:30:4c:c1:
3e:56:a3:f3:5b:76:81
ASN1 OID: secp384r1
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show pki trustpoint
Displays a PKI Certificate Authority (CA) status and its certificate.

Syntax
show pki trustpoint trustpoint-name [ status ]

Parameters
trustpoint-name
The name of the CA.

status
The status of the PKI certificate.

Modes
User EXEC mode

Examples
The following example displays the output for a CA that is not authenticated.

device# show pki trustpoint status
! CA is not authenticated, and is queried
CA Test, VRF: Default
Issuing CA certificate status: pending
Subject Name:
cn=r1 Cert Manager,ou=pki,o=company.com,c=country
Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
Router certificate status: pending
Subject Name:
hostname=host.company.com,o=company.com
Next query attempt: 52 seconds

The following example displays the output for a CA that is authenticated but the request has not started.

device# show pki trustpoint status
! CA is authenticated, and certificate request is not started
CA Test, VRF: Default
Issuing CA certificate: configured
Subject Name:
cn=r1 Cert Manager,ou=pki,o=company.com,c=country
Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
State:
Keys Generated | CA Authenticated | Certificate Request
No | Yes | None
The following example displays the output for a CA that is authenticated but the certificate request is pending.

device# show pki trustpoint status  
! CA is authenticated, and certificate request is pending  
CA Test, VRF: Default  
Issuing CA certificate: configured  
Subject Name:  
cn=r1 Cert Manager,ou=pki,o=company.com,c=country  
Fingerprint: C21514AC 12815946 09F635ED FBB6CF31  
Router Signature certificate pending:  
Requested Subject Name:  
hostname=host.company.com  
Request Fingerprint: FAE0D74E BB844EA1 54B26698 56AB42EC  
Enrollment polling: 1 times (9 left)  
Next poll: 32 seconds  
Last enrollment status: Pending  
State:  
Keys Generated | CA Authenticated | Certificate Request  
yes(signature) | Yes | Pending

The following example displays the output for a CA that is authenticated and the certificate is granted.

device# show pki trustpoint status  
! CA is authenticated, and certificate is granted  
CA Test, VRF: Default  
Issuing CA certificate: configured  
Subject Name:  
cn=r1 Cert Manager,ou=pki,o=company.com,c=country  
Fingerprint: C21514AC 12815946 09F635ED FBB6CF31  
Router Signature certificate configured:  
Subject Name:  
hostname=host.company.com,o=company.com  
Fingerprint: 8A370B8B 3B6A2464 F962178E 8385E9D6  
Router Encryption certificate configured:  
Subject Name:  
hostname=host.company.com,o=company.com  
Fingerprint: 43A03218 C0AFF844 AE0C162A 690B414A  
Last enrollment status: Granted  
State:  
Keys Generated | CA Authenticated | Certificate Request  
yes(signature) | Yes | yes

The following example displays the output for a CA trustpoint.

device# show pki trustpoint  
CA test, VRF: Default  
Subject Name:  
cn=Brocade  
o=Company  
Serial Number: 0FEEBBDC1B6F6D90EA7875875E4C695  
Certificate configured.  
Enrollment Protocol:  
SCEP, Regenerate at 80%

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show rate-limit counters bum-drop**

Displays the per-port / per-VLAN rate-limiting information for broadcast/unicast/multicast (BUM) traffic.

**Syntax**

```
show rate-limit counters bum-drop
show rate-limit counters bum-dropporport-id slot / port [ all | vlan vlan-id ]
```

**Parameters**

*port-id slot / port*
Displays the information for a specified port.

*all*
Displays the information for all BUM counters on the specified port.

*vlan vlan-id*
Displays the information for all BUM counters on the specified VLAN.

**Modes**

User EXEC mode

**Command Output**

The `show rate-limit counters bum-drop` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Displays the interface information for which the rate-limiting accounting is configured.</td>
</tr>
<tr>
<td>port: Drop:</td>
<td>Displays information about the BUM traffic (in bytes) that has been dropped as a result of the defined rate limit policy for the specific port defined.</td>
</tr>
<tr>
<td>rate-limit input broadcast</td>
<td>Displays information about the BUM traffic (in bytes) that has been dropped as a result of the defined rate limit policy.</td>
</tr>
<tr>
<td>vlan-id: 100 Drop</td>
<td>Displays information about the BUM traffic (in bytes) that has been dropped as a result of the defined rate limit policy for the specific VLAN id defined.</td>
</tr>
</tbody>
</table>
Examples

The following example for `show rate-limit counters bum-drop` command displays the following information.

Brocade(config-if-e10000-5/1)#sh rate-limit counters bum-drop

interface e 5/1
rate-limit input broadcast 993568 10000
port: Drop: 0 bytes
rate-limit input vlan-id 100 broadcast 993568 100000
vlan-id: 100 Drop: 0 bytes

Brocade(config-if-e10000-5/1)#sh rate-limit counters bum-drop port-id 5/1

interface e 5/1
rate-limit input broadcast 993568 10000
port: Drop: 0 bytes

Brocade(config-if-e10000-5/1)#sh rate-limit counters bum-drop port-id 5/1 vlan-id 100

interface e 5/1
rate-limit input vlan-id 100 broadcast 993568 100000
vlan-id: 100 Drop: 0 bytes

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show rate-limit detail

Displays detailed information for all interfaces, including the per-port / per-VLAN rate-limiting information.

Syntax

show rate-limit detail

Modes

User EXEC mode.

Examples

The show rate-limit detail command displays the following information.

Brocade#show rate-limit detail
interface e 8/1
rate-limit input vlan-id 2 broadcast multicast 97728 10000 include-control
rate-limit input broadcast multicast 97728 10000 include-control
rate-limit input access-group name ipv4_acl 100000 10000 include-control
rate-limit input access-group name ipv6_acl 100000 10000 include-control
rate-limit input access-group name ipv6_acl policy ipv6_map include-control

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show rate-limit interface**

Displays the rate-limiting information for the interface indicated.

**Syntax**

```
show rate-limit interface [ slot/port ]
```

**Modes**

User EXEC mode.

**Examples**

The `show rate-limit interface` command displays the following information.

```
Brocade#show rate-limit interface
interface e 8/1
rate-limit input vlan-id 2 broadcast multicast 97728 10000 include-control
rate-limit input broadcast multicast 97728 10000 include-control
rate-limit input access-group name ipv4_acl 100000 10000 include-control
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show rate-limit ipv6 hoplimit-expired-to-cpu**

Displays the information about rate-limit configuration on IPv6 hoplimit-not-ok packets.

**Syntax**

```
show rate-limit ipv6 hoplimit-expired-to-cpu
```

**Modes**

User EXEC mode

**Command Output**

The `show rate-limit ipv6 hoplimit-expired-to-cpu` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fwd</td>
<td>The hoplimit-expired-to-cpu traffic in bytes that has been sent to the CPU as a result of the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Drop</td>
<td>The hoplimit-expired-to-cpu traffic in bytes that has been dropped as a result of the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Re-mark</td>
<td>The hoplimit-expired-to-cpu traffic in bytes whose priority have been remarked as a result of exceed the bandwidth available in the CIR bucket for the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Total</td>
<td>The total hoplimit-expired-to-cpu traffic in bytes that has been subjected to the hoplimit-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
</tbody>
</table>

**Examples**

This example displays output of the `show rate-limit ipv6 hoplimit-expired-to-cpu` command.

```
device#show rate-limit ipv6 hoplimit-expired-to-cpu
Fwd: 1865392 Drop: 867731400 bytes
Re-mark: 1864800 Total: 871461592 bytes
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show rate-limit option-pkt-to-cpu**

Displays the information about rate-limit configuration on IPv4 option packets.

**Syntax**

```
show rate-limit option-pkt-to-cpu
```

**Modes**

User EXEC mode

**Command Output**

The `show rate-limit option-pkt-to-cpu` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fwd</td>
<td>The IPv4 option-pkt-to-cpu traffic in bytes that has been sent to the CPU as a result of the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Drop</td>
<td>The IPv4 option-pkt-to-cpu traffic in bytes that has been dropped as a result of the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Re-mark</td>
<td>The IPv4 option-pkt-to-cpu traffic in bytes whose priority have been remarked as a result of exceed the bandwidth available in the CIR bucket for the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Total</td>
<td>The total IPv4 option-pkt-to-cpu traffic in bytes that has been subjected to the IPv4 option-pkt-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
</tbody>
</table>

**Examples**

This example displays of the `show rate-limit option-pkt-to-cpu` command.

```
device# show rate-limit option-pkt-to-cpu
Fwd: 1865392 Drop: 867731400 bytes
Re-mark: 1864800 Total: 871461592 bytes
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show rate-limit ttl-expired-to-cpu

Displays the information about rate-limit configuration on IPv4 ttl-expired-to-cpu packets.

Syntax

```
show rate-limit ttl-expired-to-cpu
```

Modes

User EXEC mode

Command Output

The `show rate-limit ttl-expired-to-cpu` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fwd</td>
<td>The ttl-expired-to-cpu traffic in bytes that has been sent to the CPU as a result of the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Drop</td>
<td>The ttl-expired-to-cpu traffic in bytes that has been dropped as a result of the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Re-mark</td>
<td>The ttl-expired-to-cpu traffic in bytes whose priority have been remarked as a result of exceed the bandwidth available in the CIR bucket for the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
<tr>
<td>Total</td>
<td>The total ttl-expired-to-cpu traffic in bytes that has been subjected to the ttl-expired-to-cpu rate limit policy since the device was started up or the counter was reset.</td>
</tr>
</tbody>
</table>

Examples

This example displays output of the `show rate-limit ttl-expired-to-cpu` command.

```
device# show rate-limit ttl-expired-to-cpu
Fwd: 1865392 Drop: 867731400 bytes
Re-mark: 1864800 Total: 871461592 bytes
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show rmon alarm
Displays the Remote monitoring (RMON) alarm events.

Syntax
show rmon alarm [ number ]

Parameters
number
Specifies a RMON alarm number.

Modes
User EXEC mode

Usage Guidelines
An RMON alarm is designed to monitor configured thresholds. An alarm event is reported each time that a threshold is exceeded. The alarm entry also indicates the action (event) to be taken if the threshold be exceeded.
**show rmon statistics**

Displays the Remote monitoring (RMON) agent status and information about RMON statistics.

**Syntax**

```
show rmon statistics [ number | ethernet slot/port | management port ]
```

**Parameters**

- **number**
  
  Displays the RMON statistics for a specific statistics index identification number. Valid values range from 1 through 65535.

- **ethernet slot port**
  
  Displays the RMON statistics for a specific Ethernet interface.

- **management port**
  
  Displays the RMON statistics for a specific management port.

**Modes**

User EXEC mode

**Usage Guidelines**

Entering the `show rmon statistics` command without any options displays statistics for all ports.

**Command Output**

The `show rmon statistics` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>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.</td>
</tr>
<tr>
<td>Drop events</td>
<td>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.</td>
</tr>
<tr>
<td>Packets</td>
<td>The total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.</td>
</tr>
<tr>
<td>Broadcast pkts</td>
<td>The total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.</td>
</tr>
<tr>
<td>Multicast pkts</td>
<td>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.</td>
</tr>
<tr>
<td>CRC align errors</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Output field

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undersize pkts</td>
<td>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.</td>
</tr>
<tr>
<td>Fragments</td>
<td>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.</td>
</tr>
<tr>
<td>Oversize packets</td>
<td>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. 4BGC modules do not support count information on oversized packets and report 0.</td>
</tr>
<tr>
<td>Jabbers</td>
<td>The total number of packets received that were longer than 1518 octets and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). This number does not include framing bits but does include FCS octets. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.</td>
</tr>
<tr>
<td>Collisions</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>64 octets pkts</td>
<td>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.</td>
</tr>
<tr>
<td>65 to 127 octets pkts</td>
<td>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.</td>
</tr>
<tr>
<td>128 to 255 octets pkts</td>
<td>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.</td>
</tr>
<tr>
<td>256 to 511 octets pkts</td>
<td>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.</td>
</tr>
<tr>
<td>512 to 1023 octets pkts</td>
<td>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.</td>
</tr>
<tr>
<td>1024 to Max size</td>
<td>The total number of packets received that were 1024 octets - the maximum size of octets. This number includes bad packets. This number does not include framing bits but does include FCS octets.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays statistics for all RMON ports.

```
device(config)# show rmon statistics
Ethernet statistics 1 is active, owned by monitor
Interface 1/1 (ifIndex 1) counters
Octets          0
               Drop events          0               Packets          0
               Broadcast pkts          0               Multicast pkts          0
               CRC alignment errors          0               Undersize pkts          0
               Oversize pkts          0               Fragments          0
               Jabbers          0               Collisions          0
               64 octets pkts          0               65 to 127 octets pkts          0
               128 to 255 octets pkts          0               256 to 511 octets pkts          0
               512 to 1023 octets pkts          0               1024 to 1518 octets pkts          0
```
show route-map
Displays route map information.

Syntax
show route-map name| binding

Parameters
map-name
Shows details of the matched UDA ACL configured in the route map, along with the IPv4 ACL and IPv6 ACL.

binding
Shows the UDA PBR binding along with IPv4 and IPv6 PBR bindings. This command is supported in the LP only.

Modes
EXEC mode

Examples
The following example below shows the output of the command.

device(config)# show route-map
route-map Test1 permit 1
match uda udsAcl
match ip address 101
set next-hop-flood-vlan 10

The following example show the command using the binding option.

device# show route-map binding
IPv4 Bindings of Test1 :
  4/4
UDA PBR Bindings of Test2 :
  3/1

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to support UDA PBR information.</td>
</tr>
</tbody>
</table>
show rstp
Displays Rapid Spanning Tree Protocol (RSTP) information.

Syntax
show rstp [ blocked ] [ vlan vlan-id ]

Parameters
blocked
Displays information in respect of ports blocked by the RSTP only.

vlan vlan-id
Displays RSTP information for a specific VLAN.

Modes
User EXEC mode

Usage Guidelines
This command can also be entered in global configuration mode.

Examples
The following example displays a summary of RSTP information for VLAN 10:

device> show rstp vlan 10
VLAN 10 - RSTP instance 0
-----------------------------------------------------------
RSTP (IEEE 802.1w) Bridge Parameters:
Bridge Identifier MaxAge Hello FwdDly Version Hold
hex sec sec sec cnt
0001000480a04000 20 2 2 15 Default 3
RootBridge Identifier RootPath DesignatedBridge Root Max Hel Fwd
hex hex hex sec sec sec
0001000480a04000 0 0001000480a04000 Root 20 2 15
RSTP (IEEE 802.1w) Port Parameters:
<--- Config Params -->|<------------------- Current state ------------------->
Port Pri PortPath P2P Edge Role State Designated Designated
Num Cost Mac Port ted cost bridge
1/3 128 20000 T F DISABLED DISABLED 0 0000000000000000
1/13 128 20000 T F DISABLED DISABLED 0 0000000000000000
The following example displays a summary of ports blocked by RSTP on VLAN 20:

device> show rstp blocked vlan 20

VLAN 20 - RSTP instance 0
---------------------------------
RSTP (IEEE 802.1w) Bridge Parameters:

RSTP (IEEE 802.1w) Port Parameters:

<--- Config Params -->|<-------------- Current state ----------------->

<table>
<thead>
<tr>
<th>Port Num</th>
<th>Pri Cost</th>
<th>PortPath Mac Port</th>
<th>P2P</th>
<th>Edge</th>
<th>Role</th>
<th>State</th>
<th>Designated cost</th>
<th>Designated bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/6</td>
<td>128 2000</td>
<td>F F</td>
<td>F</td>
<td>F</td>
<td>ALTERNATE</td>
<td>DISCARDING</td>
<td>0</td>
<td>80000024388f6b20</td>
</tr>
<tr>
<td>3/7</td>
<td>128 2000</td>
<td>F F</td>
<td>F</td>
<td>F</td>
<td>ALTERNATE</td>
<td>DISCARDING</td>
<td>0</td>
<td>80000024388f6b20</td>
</tr>
<tr>
<td>3/8</td>
<td>128 2000</td>
<td>F F</td>
<td>F</td>
<td>F</td>
<td>ALTERNATE</td>
<td>DISCARDING</td>
<td>0</td>
<td>80000024388f6b20</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>The command was modified to display only ports blocked by the RSTP.</td>
</tr>
</tbody>
</table>
show running-config
Displays the current running configuration.

Syntax
show running-config

Parameters
interface
Displays the running-configuration section.
ethernet slot/port
Displays the specified ethernet port.
loopback num
Displays the loopback port.
pos slot/port
Displays the specified POS port.
tunnel num
Displays the specified tunnel port.
ve num
Displays the specified Virtual Ethernet (VE) port.
lag
Displays the LAG running-configuration section.
detailed
Displays the LAG running-configuration information in detail.
id lag_id
Displays the specified LAG running-configuration.
name lag_name
Displays the specified LAG running-configuration name.

Modes
User EXEC mode

Usage Guidelines
Use this command with filtering for the specific command for which you want to review the current configuration on the device. Most commands are available in this format using either the begin or the include options. See the Example section for examples of each option.
Examples

The following example displays the `show running-config` command. Notice that the interface bandwidth command is displayed as part of the interface configuration.

```
device#show running-config interface tunnel 2
interface tunnel 2
    tunnel mode gre ip
    tunnel source 169.70.15.2
    tunnel destination 169.70.15.1
    ip address 199.0.0.2/24
    bandwidth 2000
```

The following example displays the `show running-config` command executed on an Ethernet interface.

```
device#show running-config interface ethernet 8/1
interface e 8/1
    rate-limit input vlan-id 2 broadcast multicast 97728 10000 include-control
    rate-limit input broadcast multicast 97728 10000 include-control
    rate-limit input access-group name ipv4_acl 100000 10000 include-control
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was modified to include the interface bandwidth command as part of the interface configuration.</td>
</tr>
</tbody>
</table>
show sflow statistics

Displays the total count per interface for both sFlow and ACL-based samples in all slots where sFlow is configured.

Syntax

```
show sflow statistics slot/port
```

Parameters

- `slot port` Displays statistics for the specified port.

Modes

- User EXEC mode

Usage Guidelines

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to display sFlow statistics information.</td>
</tr>
</tbody>
</table>
show spanning-tree

Displays Spanning Tree Protocol (STP) information.

Syntax

```
show spanning-tree [ blocked ] [ vlan vlan-id [ ethernet slot/port ] ]
```

Parameters

- **blocked**
  - Displays information for ports blocked by the STP only.

- **vlan vlan-id**
  - Displays information for a specific port-based VLAN.

- **ethernet slot port**
  - Displays information for a specific Ethernet interface on a port-based VLAN.

Modes

- User EXEC mode

Usage Guidelines

This command is also available in global configuration mode.

Examples

The following example displays STP information for VLAN 10:

```
device> show spanning-tree vlan 10
```

```
VLAN 10 - STP instance 1
---------------------------------------------------------------
STP Bridge Parameters:
Bridge Identifier MaxAge Hello FwdDly Time Change Change
hex 8000000480a04000 20 2 15 1 0 0
RootBridge Identifier RootPath DesignatedBridge Root Max Hel Fwd
hex 8000000480a04000 Root 0 0 0
STP Port Parameters:
Port Prio Path State Designat- Designated Designated
Num rity Cost ed Cost Root Bridge
1/3 128 4 DISABLED 0 0000000000000000 0000000000000000
1/13 128 4 DISABLED 0 0000000000000000 0000000000000000
```
The following example displays STP information for VLAN 10, listing blocked ports only:

device> show spanning-tree blocked vlan 10

VLAN 10 - STP instance 0

STP Bridge Parameters:

<table>
<thead>
<tr>
<th>Bridge Identifier</th>
<th>Bridge MaxAge</th>
<th>Bridge Hello</th>
<th>Bridge FwdDly</th>
<th>Bridge Time</th>
<th>Bridge Change</th>
<th>Bridge Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex 80000024389e2d00</td>
<td>20 sec</td>
<td>2 sec</td>
<td>15 sec</td>
<td>1 sec</td>
<td>718 sec</td>
<td>1 cnt</td>
</tr>
</tbody>
</table>

RootBridge Parameters:

<table>
<thead>
<tr>
<th>RootBridge Identifier</th>
<th>RootBridge RootPath</th>
<th>RootBridge DesignatedBridge Identifier</th>
<th>RootBridge Root</th>
<th>RootBridge Max</th>
<th>RootBridge Hel</th>
<th>RootBridge Fwd</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex 80000024388f6b00</td>
<td>2 port</td>
<td>80000024388f6b00</td>
<td>3/1 port</td>
<td>20 sec</td>
<td>2 sec</td>
<td>15 sec</td>
</tr>
</tbody>
</table>

STP Port Parameters:

<table>
<thead>
<tr>
<th>Port Num</th>
<th>Port Priority</th>
<th>Port Path</th>
<th>Port State</th>
<th>Port Designat-Edge Cost</th>
<th>Port Designated Cost</th>
<th>Port Designated RootBridge Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/2</td>
<td>128</td>
<td>2</td>
<td>BLOCKING</td>
<td>0</td>
<td>80000024388f6b00</td>
<td>80000024388f6b00</td>
</tr>
<tr>
<td>3/3</td>
<td>128</td>
<td>2</td>
<td>BLOCKING</td>
<td>0</td>
<td>80000024388f6b00</td>
<td>80000024388f6b00</td>
</tr>
<tr>
<td>3/4</td>
<td>128</td>
<td>2</td>
<td>BLOCKING</td>
<td>0</td>
<td>80000024388f6b00</td>
<td>80000024388f6b00</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>The command was modified to display only ports blocked by the Spanning Tree Protocol.</td>
</tr>
</tbody>
</table>
**show statistics**
Displays the statistics for a specific option.

**Syntax**

```
show statistics brief [ ethernet | lag | management | pos | slot | tunnel ]
show statistics dos-attack
show statistics ethernet slot/port
show statistics lag lag_name
show statistics management dec
show statistics pos slot/port
show statistics slot dec
show statistics tunnel tunnel-id
show statistics ipsec-tunnel tunnel-id
```

**Parameters**

- **brief**
  Displays the port statistics in brief mode.

- **ethernet**
  Displays the ethernet port in brief mode.

- **lag**
  Displays LAG in brief mode.

- **management**
  Displays the management port in brief mode.

- **pos**
  Displays the POS port in brief mode.

- **slot**
  Displays all ports in a slot in brief mode.

- **tunnel**
  Displays IP tunnel statistics in brief mode.

- **dos-attack**
  Displays DOS-attack statistics.

- **ethernet slot/port**
  Displays the ethernet port for the specified slot and port.

- **lag**
  Displays LAG determined by the lag_name variable.

- **management**
Displays the management port determined by the `dec` variable.

**pos**

Displays the POS port determined by the `slot/port` variable.

**slot**

Displays all of the ports in a slot determined by the `slot/port` variable.

**tunnel**

Displays the IP tunnel statistics determined by the `tunnel-id` variable.

**ipsec-tunnel** `tunnel-id`

Displays the bytes and packets count for the specified IPSec tunnel ID.

**Modes**

This command operates under all modes.

**Command Output**

The `show statistics ethernet` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOctets</td>
<td>The total number of good octets and band octets received.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>The total number of good and bad octets transmitted.</td>
</tr>
<tr>
<td>InPkts</td>
<td>The total number of packets received. the count includes rejected and local packets that are not transmitted to the switching core for transmission.</td>
</tr>
<tr>
<td>OutPkts</td>
<td>The number of good packets received. The count includes unicast, multicast, and broadcast packets.</td>
</tr>
<tr>
<td>InBroadcastPkts</td>
<td>The total number of good broadcast packets received.</td>
</tr>
<tr>
<td>OutBroadcastPkts</td>
<td>The total number of good broadcast packets transmitted.</td>
</tr>
<tr>
<td>InMulticastPkts</td>
<td>The total number of good multicast packets received.</td>
</tr>
<tr>
<td>OutMulticastPkts</td>
<td>The total number of good multicast packets transmitted.</td>
</tr>
<tr>
<td>InUnicastPkts</td>
<td>The total number of good unicast packets received.</td>
</tr>
<tr>
<td>OutUnicastPkts</td>
<td>The total number of good unicast packets transmitted.</td>
</tr>
<tr>
<td>InDiscards</td>
<td>The total number of packets that were received and then dropped due to a lack of received buffers.</td>
</tr>
<tr>
<td>OutDiscards</td>
<td>The total number of packets that were transmitted and then dropped due to a lack of transmit buffers.</td>
</tr>
<tr>
<td>InErrors</td>
<td>The total number of packets received that had Alignment errors or phy errors.</td>
</tr>
<tr>
<td>OutErrors</td>
<td>The total number of packets transmitted that has Alignment errors or phy errors.</td>
</tr>
<tr>
<td>InCollisions</td>
<td>The total number of packets received in which a Collision event was detected.</td>
</tr>
<tr>
<td>OutCollisions</td>
<td>The total number of packets transmitted in which a Collision event was detected.</td>
</tr>
<tr>
<td>OutLateCollisions</td>
<td>The total number of packets transmitted in which a Collision event was detected but for which a receive error (RX error) event was not detected.</td>
</tr>
<tr>
<td>Alignment</td>
<td>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).</td>
</tr>
<tr>
<td>FCS</td>
<td>The Frame Checksum error.</td>
</tr>
</tbody>
</table>
### Output field | Description
---|---
InFlowCtrlPkts | The total number of ingress flow control packets. "N/A" indicates that the interface module does not support flow control statistics.
OutFlowCtrlPkts | The total number of egress flow control packets.
GiantPkts | The total number of packets for which all of the following is true:
- The data length was longer than the maximum allowable frame size.
- No Rx error was detected.
ShortPkts | The total number of packets received for which all of the following is true:
- The data length was less than 64 bytes.
- No Rx error was detected.
- No Collision or late Collision was detected.
InBitsPerSec | The number of bits received per second.
OutBitsPerSec | The number of bits transmitted per second.
InPktsPerSec | The number of packets received per second.
OutPktsPerSec | The number of packets transmitted per second.
InUtilization | The percentage of the port's bandwidth used by received traffic.
OutUtilization | The percentage of the port's bandwidth used by transmitted traffic.

The **show statistics tunnel** command displays the following information:

<table>
<thead>
<tr>
<th>This field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel ID</td>
<td>For each tunnel displayed, the Tunnel ID indicates the tunnel for which the statistics are displayed.</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>The tunnel type is either GRE or manual IPv6.</td>
</tr>
<tr>
<td>In-ports</td>
<td>The Ethernet ports traversed by the tunnel.</td>
</tr>
<tr>
<td>Packets Rcv-from-tnnl</td>
<td>The number of packets that have arrived from the tunnel.</td>
</tr>
<tr>
<td>Packets Xmit-to-tnnl</td>
<td>The number of packets that have been sent to the tunnel.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the **show statistics ethernet** command:

```
device# show statistics ethernet 9/1
```

**PORT 9/1 Counters:**

<table>
<thead>
<tr>
<th>InOctets</th>
<th>210753498112</th>
<th>OutOctets</th>
<th>210753550720</th>
</tr>
</thead>
<tbody>
<tr>
<td>InPkts</td>
<td>1646511726</td>
<td>OutPkts</td>
<td>1646512119</td>
</tr>
<tr>
<td>InBroadcastPkts</td>
<td>0</td>
<td>OutBroadcastPkts</td>
<td>0</td>
</tr>
<tr>
<td>InMulticastPkts</td>
<td>0</td>
<td>OutMulticastPkts</td>
<td>0</td>
</tr>
<tr>
<td>InUnicastPkts</td>
<td>1646511726</td>
<td>OutUnicastPkts</td>
<td>1646512142</td>
</tr>
<tr>
<td>InDiscards</td>
<td>0</td>
<td>OutDiscards</td>
<td>0</td>
</tr>
<tr>
<td>InErrors</td>
<td>0</td>
<td>OutErrors</td>
<td>0</td>
</tr>
<tr>
<td>InCollisions</td>
<td>0</td>
<td>OutCollisions</td>
<td>0</td>
</tr>
<tr>
<td>OutLateCollisions</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alignment</td>
<td>0</td>
<td>PCS</td>
<td>0</td>
</tr>
<tr>
<td>InFlowCtrlPkts</td>
<td>0</td>
<td>OutFlowCtrlPkts</td>
<td>0</td>
</tr>
<tr>
<td>GiantPkts</td>
<td>0</td>
<td>ShortPkts</td>
<td>0</td>
</tr>
<tr>
<td>InBitsPerSec</td>
<td>3440829770</td>
<td>OutBitsPerSec</td>
<td>3440686411</td>
</tr>
<tr>
<td>InPktsPerSec</td>
<td>3360185</td>
<td>OutPktsPerSec</td>
<td>3360085</td>
</tr>
<tr>
<td>InUtilization</td>
<td>39.78%</td>
<td>OutUtilization</td>
<td>39.78%</td>
</tr>
</tbody>
</table>
The following example displays output from the `show statistics tunnel` command with a specific `tunnel-id` option. In this example, the tunnel type is GRE.

**NOTE**
When reviewing the keepalive packet statistics in the output of the `show interface tunnel` command for a GRE tunnel, note that the transmitted keepalive packets are hardware generated and are not counted in the “Rcv-from-tnnl” and “Xmit-to-tnnl” statistics.

```
device# show statistics tunnel 1
Packets
Tunnel Id  Tunnel Type  In-Port(s)  [Rcv-from-tnnl  Xmit-to-tnnl]
1         GRE          e2/1 - e2/2  586046           287497
           e2/3 - e2/4  100340           150034
```

The following example displays the `show statistics brief ipsec-tunnel` command modified to display IPsec tunnel interface packet and byte count.

```
device# show statistics brief ipsec-tunnel
   #   Tnnl   RxPkts  RxBytes  TxPkts  TxBytes
   1    24     0       0       0       0
   2    100    0       0       457     79518
   3    101    0       0       0       0
   4    102    0       0       0       0
   5    103    0       0       1       174
   6    104    0       0       0       0
   7    105    0       0       0       0
   8    106    0       0       0       0
   9    107    0       0       0       0
  10    108    0       0       0       0
  11    109    0       0       0       0
  12    110    0       0       0       0
  13    123    0       0       0       0
  14    124    0       0       0       0
  15    125    0       0       0       0
  16    150    0       0       0       0
  17    254    0       0       0       0
```

The following example shows the bytes and packet count only for the IPsec tunnel interface 100.

```
device# show statistics ipsec-tunnel 100
IPSec tunnel 100 statistics:
RxPkts: 0
RxBytes: 0
TxPkts: 467
TxBytes: 81258
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was modified to display IPsec tunnel interface packet and byte count.</td>
</tr>
</tbody>
</table>
**show sysmon config**

Displays the system monitoring configuration.

**Syntax**

```
show sysmon config
```

**Modes**

User EXEC mode

**Command Output**

The `show sysmon config` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVENT</td>
<td>Name of the diagnostic test.</td>
</tr>
<tr>
<td>ACTION</td>
<td>Action to be taken in case of a failure of the test.</td>
</tr>
<tr>
<td>POLL PERIOD (SEC)</td>
<td>The polling period in seconds.</td>
</tr>
<tr>
<td>THRESHOLD #(PER POLL in #POLL)</td>
<td>The number of failed tests out of the number of pollings (applicable only for threshold based test).</td>
</tr>
<tr>
<td>LOG BACK-OFF</td>
<td>The number of event logs to be skipped before logging again.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the monitoring configuration.

```
device# show sysmon config
```

<table>
<thead>
<tr>
<th>EVENT</th>
<th>ACTION</th>
<th>POLL PERIOD (SEC)</th>
<th>THRESHOLD #(PER POLL in #POLL)</th>
<th>LOG BACK-OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>TM. Link Monitoring</td>
<td>SHUTDOWN-LINK</td>
<td>60</td>
<td>5 in 10</td>
<td>1800</td>
</tr>
<tr>
<td>Port CRC Monitoring</td>
<td>SYSLOG</td>
<td>60</td>
<td>3 in 5</td>
<td>1800</td>
</tr>
<tr>
<td>FE. Link Monitoring</td>
<td>SHUTDOWN-LINK</td>
<td>60</td>
<td>5 in 10</td>
<td>1800</td>
</tr>
<tr>
<td>NP Memory Error Monitoring</td>
<td>SYSLOG-AND-TRAP</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**History**

<table>
<thead>
<tr>
<th>Release Version</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was modified to display the NP memory error monitoring event configuration.</td>
</tr>
</tbody>
</table>
show sysmon results brief

Displays summary information of scheduled test results in brief without providing the instance information.

Syntax

```
show sysmon results test-name brief
```

Parameters

`test-name`

Displays summary results for a specific scheduled test.

Modes

User EXEC mode

Command Output

The `show sysmon results brief` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVENT</td>
<td>Name of the diagnostic test.</td>
</tr>
<tr>
<td>ACTION</td>
<td>Action to be taken in case of a failure of the test.</td>
</tr>
<tr>
<td>SLOTS</td>
<td>Slots on which the test is configured to run.</td>
</tr>
<tr>
<td>MODE</td>
<td>Mode of running for the test. The modes are Continuously polling or Scheduling.</td>
</tr>
<tr>
<td>POLL PERIOD (SEC)</td>
<td>The polling period in seconds.</td>
</tr>
<tr>
<td>THRESHOLD #(PER POLL in #POLL)</td>
<td>The number of failed tests out of the number of pollings (applicable only for threshold based test).</td>
</tr>
<tr>
<td>LOG BACK-OFF</td>
<td>The number of event logs to be skipped before logging again.</td>
</tr>
<tr>
<td>SLOT</td>
<td>The slot number.</td>
</tr>
<tr>
<td>TEST TYPE</td>
<td>The specific scheduling test type.</td>
</tr>
<tr>
<td>BRIEF RESULT (LAST RUN/CYCLE)</td>
<td>The brief results showing only the status (passed/ failed) of the test on each slot.</td>
</tr>
</tbody>
</table>
Examples

The following example displays results from the port-crc-test:

device(config)#show sysmon results port-crc-test brief
Module is(are) not UP in slot(s) 3 4 5

The configuration of port-crc-test is

+-------------------------+---------------------+----------+----------+-----------+------------+
| EVENT                    | ACTION               | SLOTS     | MODE      | POLL PERIOD| THRESHOLD  |
|                          |                      |          |           |            | in #POLL   |
|                          |                      |          |           |   (SEC)    | (PER POLL |
|                          |                      |          |           | in #POLL)  |
|-------------------------+---------------------+----------+----------+-----------+------------+
| Port CRC Monitoring      | SYSLOG               | ALL      | SCHEDULING|     60    |   3 in 4   |

Brief result of port-crc-test is

+-------------------------+---------------------------------------+------------------------------------+
<table>
<thead>
<tr>
<th>SLOT</th>
<th>TEST TYPE</th>
<th>BRIEF RESULT (LAST RUN/CYCLE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot 1</td>
<td>Scheduled at  2014.05.27-10:56:52</td>
<td>PASSED</td>
</tr>
<tr>
<td>Slot 2</td>
<td>Scheduled at  2014.05.27-10:56:52</td>
<td>PASSED</td>
</tr>
<tr>
<td>Slot 6</td>
<td>Scheduled at  2014.05.27-10:56:52</td>
<td>PASSED</td>
</tr>
<tr>
<td>Slot 7</td>
<td>Scheduled at  2014.05.27-10:56:52</td>
<td>PASSED</td>
</tr>
<tr>
<td>Slot 8</td>
<td>Scheduled at  2014.05.27-10:56:52</td>
<td>PASSED</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show sysmon results detail**

Displays scheduled test results in detail for a specified slot. Instance information and other details are displayed.

**Syntax**

```
show sysmon results test-name detail slot-id
```

**Parameters**

- **test-name**
  Displays detailed results for specified test name.

- **slot-id**
  Displays detailed results for a specified slot name of the slot numbers to be specified to run the test.

**Modes**

User EXEC mode

**Command Output**

The `show sysmon results detail` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVENT</td>
<td>Name of the diagnostic test.</td>
</tr>
<tr>
<td>ACTION</td>
<td>Action to be taken in case of a failure of the test.</td>
</tr>
<tr>
<td>SLOTS</td>
<td>Slots on which the test is configured to run.</td>
</tr>
<tr>
<td>MODE</td>
<td>Mode of running for the test. The modes are Continuously polling or Scheduling.</td>
</tr>
<tr>
<td>POLL PERIOD (SEC)</td>
<td>The polling period in seconds.</td>
</tr>
<tr>
<td>THRESHOLD #(PER POLL in #POLL)</td>
<td>The number of failed tests out of the number of pollings (applicable only for threshold based test).</td>
</tr>
<tr>
<td>LOGBACK-OFF</td>
<td>The number of event logs to be skipped before logging again.</td>
</tr>
<tr>
<td>INSTANCE</td>
<td></td>
</tr>
<tr>
<td>TEST TYPE</td>
<td>The specific scheduling test type.</td>
</tr>
<tr>
<td># OF RUNS</td>
<td>The number of times test is run.</td>
</tr>
<tr>
<td># OF FAILURES</td>
<td>The number of times the test failed (out of the number of runs).</td>
</tr>
</tbody>
</table>
Examples

The following example displays information about the port-crc-test.

```
device(config)#show sysmon results port-crc-test detail 1
```

The configuration of port-crc-test is

```
+---------------------------+---------------------+-------------+----------+-----------+------------|
<table>
<thead>
<tr>
<th>EVENT</th>
<th>ACTION</th>
<th>SLOTS</th>
<th>MODE</th>
<th>POLL PERIOD</th>
<th>THRESHOLD</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGBACK-OFF</td>
<td></td>
<td></td>
<td></td>
<td>(SEC)</td>
<td>#(PER POLL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>in #POLL)</td>
<td></td>
</tr>
</tbody>
</table>
+---------------------------+---------------------+-------------+----------+-----------+------------|
| Port CRC Monitoring       | SYSLOG              | ALL         | SCHEDULING|     60    |   3 in 4   |
+---------------------------+---------------------+-------------+----------+-----------+------------|
```

The detail result (LAST RUN/CYCLE) of port-crc-test on LP 1 is

```
+------------------+-----------------------------------+--------+---------|
| INSTANCE         | TYPE                              | # OF   | # OF    |
| Port 1/1         | Scheduled at 2014.05.27-10:56:52  | 4      | 0       |
| Port 1/2         | Scheduled at 2014.05.27-10:56:52  | 4      | 0       |
| Port 1/3         | Scheduled at 2014.05.27-10:56:52  | 4      | 0       |
| Port 1/4         | Scheduled at 2014.05.27-10:56:52  | 4      | 0       |
+------------------+-----------------------------------+--------+---------|
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show sysmon schedule
Displays details of scheduled tests.

Syntax
show sysmon sched name of the test

Parameters
name of the test
The name of the scheduled test.

Modes
User EXEC mode
Privileged EXEC mode
Global configuration mode

Command Output
The show sysmon schedule command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEST NAME</td>
<td>Name of the test.</td>
</tr>
<tr>
<td>SCHEDULED AT</td>
<td>The scheduled time in hh:mm:ss mm-dd-yy format. Here the first instance of mm is minutes and the second instance is months. For example, 14:30:00 08-20-13.</td>
</tr>
<tr>
<td>MP/LP</td>
<td>Type of slot.</td>
</tr>
<tr>
<td># OF RUNS</td>
<td>The number of runs. The range is between 1 and 31.</td>
</tr>
<tr>
<td>THRESHOLD</td>
<td>Threshold value of the diagnostic test.</td>
</tr>
<tr>
<td>TEST INTERVAL (SEC)</td>
<td>The test interval value in seconds.</td>
</tr>
</tbody>
</table>

Examples
The following example displays information about the port-crc-test.

device(config)#show sysmon schedule port-crc-test

<table>
<thead>
<tr>
<th>TEST NAME</th>
<th>SCHEDULED AT</th>
<th>MP/LP</th>
<th># OF RUNS</th>
<th>THRESHOLD</th>
<th>TEST INTERVAL (SEC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port CRC Monitoring</td>
<td>2014.05.23-06:39:28</td>
<td>LP</td>
<td>4</td>
<td>3</td>
<td>60</td>
</tr>
</tbody>
</table>
The following example displays information about the np-memory-errors test.

device(config)#show sysmon schedule np-memory-errors

<table>
<thead>
<tr>
<th>TEST NAME</th>
<th>SCHEDULED</th>
<th>MP/LP</th>
<th># OF RUNS</th>
<th>THRESHOLD</th>
<th>TEST INTERVAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NP Memory Error Monitoring</td>
<td>2014.05.23-06:39:34</td>
<td>LP</td>
<td>4</td>
<td>0</td>
<td>60</td>
</tr>
</tbody>
</table>

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
show telemetry
Displays information related to the telemetry configuration.

Syntax
show telemetry [ detail ] rule-name rule-name

Parameters
detail
Displays detailed information. The list of ports will be fully expanded and displayed if the ports are LAG or VLAN ports.

rule-name rule-name
Displays specified rule name information.

Modes
EXEC mode

Usage Guidelines

Examples
The following example displays the UDA PBR policy detail along with the IPv4, IPv6 PBR information.

device(config)# show telemetry detail rule-name
Rule name: default-rulename
Input: IPv4 - 1/1
Route-map Policy: Test2
IPv4 ACL match: 110
Output:
Input: IPv4 - 3/1
Route-map Policy: Test1
IPv4 ACL match: 100
Output:
Input: UDA - 3/1
Route-map Policy: Test1
UDA ACL match: 2000
Output:

The following example displays the UDA PBR policy detail along with the IPv4, IPv6 and PBR information.

device(config)# show telemetry rule-name
Paths with leading * are configured but disabled, entries with + are for IPv6 entries with # are for UDA

<table>
<thead>
<tr>
<th>Name</th>
<th>Input</th>
<th>Route-map</th>
<th>ACL</th>
<th>Match</th>
<th>VLAN</th>
<th>Output</th>
<th>Port(s)/IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>RT_TEST1</td>
<td>4/8</td>
<td>Test1</td>
<td></td>
<td></td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+RT_TEST1</td>
<td>4/8</td>
<td>Test1</td>
<td></td>
<td></td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#RT_TEST1</td>
<td>4/8</td>
<td>Test1</td>
<td></td>
<td></td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*RT_TEST3</td>
<td>N/A</td>
<td>Test3</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#RT_TEST4</td>
<td>3/3</td>
<td>Test4</td>
<td></td>
<td></td>
<td>2/3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Release version

5.9.00 This command was modified to display the UDA PBR policy detail along with the IPv4, IPv6 PBR information.
**show terminal**
Displays terminal settings.

**Syntax**

```
show terminal
```

**Modes**

User EXEC mode

**Command Output**

The `show terminal` command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-08-11T22:20:59+00:00</td>
<td>Timestamp is displayed in ISO 8601 format: YYYY-MM-DDThh:mm:ssTZD (for example, 1997-07-16T19:20:30+01:00).</td>
</tr>
<tr>
<td>Length</td>
<td>Number of lines configured as the terminal length.</td>
</tr>
<tr>
<td>Page display mode (session)</td>
<td>Session page display is either enabled or disabled.</td>
</tr>
<tr>
<td>Page display mode (global)</td>
<td>Global page display is either enabled or disabled.</td>
</tr>
<tr>
<td>Timestamp: enabled</td>
<td>The format in which the timestamp is displayed; system or iso8601.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the terminal settings.

```
device# show terminal
```

```
Length: 24 lines
Page display mode (session): disabled
Page display mode (global): enabled
Timestamp: enabled (system format)
```

The following example displays the terminal settings with a timestamp and iso8601 format.

```
device# show terminal
```

```
2015-08-11T22:20:59+00:00
Length: 24 lines
Page display mode (session): disabled
Page display mode (global): enabled
Timestamp: enabled (iso8601 format)
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.4.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.9.0</td>
<td>This command was modified to include timestamp information in ISO 8601 format.</td>
</tr>
</tbody>
</table>
show tm-voq-stat queue-drops

Use `show tm-voq-stat queue-drops` command to display traffic manager statistics.

**Syntax**

```
show tm-voq-stat queue-drops dst_port destination-port ethernet slot/port
```

**Modes**

This command operates in the Global configuration mode.

**Command Output**

The `show tm-voq-stat queue-drops` command displays the following information:

**TABLE 11 Traffic Manager statistics for queue drops**

<table>
<thead>
<tr>
<th>This field</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnQue Pkt Count</td>
<td>A count of all packets entering ingress queues on this traffic manager.</td>
</tr>
<tr>
<td>EnQue Byte Count</td>
<td>A count of all bytes entering ingress queues on this traffic manager.</td>
</tr>
<tr>
<td>DeQue Pkt Count</td>
<td>A count of all packets dequeued from ingress queues and forwarded on this traffic manager.</td>
</tr>
<tr>
<td>DeQue Byte Count</td>
<td>A count of all bytes dequeued from ingress queues and forwarded on this traffic manager.</td>
</tr>
<tr>
<td>TotalQue Discard Pkt Count</td>
<td>A count of all packets failing to enter ingress queues on this traffic manager. This may be due to:</td>
</tr>
<tr>
<td></td>
<td>• the queue reaching its maximum depth, WRED, or other reasons.</td>
</tr>
<tr>
<td></td>
<td>• the network processor deciding to drop packets for reasons including: an unknown Layer-3 route, RPF, or segment filtering.</td>
</tr>
<tr>
<td>TotalQue Discard Byte Count</td>
<td>A count of all bytes failing to enter ingress queues on this traffic manager. This may be due to:</td>
</tr>
<tr>
<td></td>
<td>• the queue reaching its maximum depth, WRED, or other reasons.</td>
</tr>
<tr>
<td></td>
<td>• the network processor deciding to drop packets for reasons including: an unknown Layer-3 route, RPF, or segment filtering.</td>
</tr>
</tbody>
</table>

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>NI 5.7.00 release</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>
show tvf-domain
Displays transparent VLAN flooding (TVF) domain information.

Syntax
show tvf-domain [ tvf-domain-ID | brief | detail | ethernet slot/port ]

Parameters
- tvf-domain-ID
  Displays the information of a specific TVF domain.
- brief
  Displays a brief summary of all the configured TVF domains.
- detail
  Displays detailed information of each TVF domain.
- ethernet slot/port
  Displays the details of the port configured in the VLAN.

Modes
- Privileged EXEC mode
- Global configuration mode
- Interface configuration mode
- TVF domain configuration mode

Command Output
The show tvf-domain command displays the following information:

<table>
<thead>
<tr>
<th>Output field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TVF FID pool size</td>
<td>FID pool size configured for TVF LAG load balancing.</td>
</tr>
<tr>
<td>Max FID groups</td>
<td>Maximum number of FID groups.</td>
</tr>
<tr>
<td>FID group size</td>
<td>FID group size configured for TVF LAG load balancing.</td>
</tr>
<tr>
<td>TVF domain memory usage</td>
<td>Transparent VLAN flooding memory usage.</td>
</tr>
<tr>
<td>Per entry usage</td>
<td>Memory usage for each entry.</td>
</tr>
<tr>
<td>TVF Domain ID</td>
<td>ID of the TVF domain.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the TVF domain</td>
</tr>
<tr>
<td>Ports</td>
<td>Ports configured in the VLAN.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of ports.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Supported protocols. Value is NONE as protocol support is not added.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the port.</td>
</tr>
<tr>
<td>Group ID</td>
<td>LAG trunk ID.</td>
</tr>
</tbody>
</table>
### Output field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FID Base</td>
</tr>
<tr>
<td>FID Count</td>
</tr>
</tbody>
</table>

### Examples

The following example displays information about the TVF domain.

```plaintext
device(config)# show tvf-domain
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 2048, FID group size: 2
2047 (VLAN 32, TVF Domain 2015) TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done

TVF domain memory usage : 735848 bytes
Per entry usage : 365 bytes

TVF Domain ID 1, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 2, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 3, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 4, Name [None]
Ports : ethe 8/5 to 8/8

TVF Domain ID 6, Name [None]
Ports : ethe 8/5 to 8/8
```

The following example displays the information of a specific TVF domain.

```plaintext
device(config)# show tvf-domain 1
TVF Domain ID 1, Name [None]
Ports : ethe 8/5 to 8/8

-----------------------------------------------
Port  Type  Protocol  State
8/5  TRUNK     NONE     UP
8/6  TRUNK     NONE     UP
8/7  TRUNK     NONE     UP
8/8  TRUNK     NONE     UP
-----------------------------------------------
Group ID: 33, FID Base 0x00009ffe, FID Count 2
tvf_lag_lb_fid0: 0x00009ffe, mask ethe 8/5 ethe 8/7
tvf_lag_lb_fid1: 0x00009fff, mask ethe 8/6 ethe 8/8
```
The following example displays a brief summary of all the configured TVF domains.

device(config)# show tvf-domain brief

**** TVF LAG Load Balancing ****

TVF LAG Load Balancing is enabled!

TVF FID pool size: 4096, Max FID groups: 2048, FID group size: 2

2047 (VLAN 32, TVF Domain 2015) TVF LAG Load balancing groups are configured

TVF LAG Load balancing FID programming is done

TVF domain memory usage : 735848 bytes
Per entry usage : 365 bytes

<table>
<thead>
<tr>
<th>TVF</th>
<th>Name</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>2</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>3</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>4</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>5</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>6</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>7</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>8</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>9</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>10</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>11</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>12</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>13</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>14</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>15</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>16</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>17</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>18</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>19</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>20</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>21</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>22</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>23</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>24</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>25</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>26</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>27</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>28</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>29</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>30</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>31</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>32</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>33</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>34</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>35</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>36</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
<tr>
<td>37</td>
<td>[None]</td>
<td>Ports : ethe 8/5 to 8/8</td>
</tr>
</tbody>
</table>
The following example displays detailed information of each TVF domain.

device(config)# show tvf-domain detail
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 2048, FID group size: 2
2047 (VLAN 32, TVF Domain 2015) TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done

TVF domain memory usage : 735848 bytes
Per entry usage : 365 bytes

TVF Domain ID 1, Name [None]
Ports : ethe 8/5 to 8/8
----------------------------------------------------------
Port  Type      Protocol  State
8/5   TRUNK     NONE      UP
8/6   TRUNK     NONE      UP
8/7   TRUNK     NONE      UP
8/8   TRUNK     NONE      UP
Group ID: 34, FID Base 0x00009ffe, FID Count 2

TVF Domain ID 2, Name [None]
Ports : ethe 8/9 to 8/12
----------------------------------------------------------
Port  Type      Protocol  State
8/9   TRUNK     NONE      UP
8/10   TRUNK     NONE      UP
8/11   TRUNK     NONE      UP
8/12   TRUNK     NONE      UP
Group ID: 33, FID Base 0x00009ffe, FID Count 2

The following example displays the details of the port configured in the TVF domain.

device(config)# show tvf-domain ethernet 8/6
TVF Domain : 1
TVF Domain : 2
TVF Domain : 3
TVF Domain : 4
TVF Domain : 6
TVF Domain : 7
TVF Domain : 8
TVF Domain : 9
TVF Domain : 10
TVF Domain : 11
TVF Domain : 12
TVF Domain : 13
TVF Domain : 14
TVF Domain : 15
TVF Domain : 16
TVF Domain : 17
TVF Domain : 18
TVF Domain : 19
TVF Domain : 20
TVF Domain : 21
TVF Domain : 22
TVF Domain : 23
TVF Domain : 24

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**show vlan**

Displays VLAN information.

**Syntax**

```
show vlan vlan_id [ statistics ]
show vlan vlan_id brief [ wide ]
show vlan vlan_id [ statistics ] detail
show vlan vlan_id [ statistics ] ethernet [ slot/port ]
show vlan vlan_id [ statistics ] tvf-lag-lb [ detail ]
```

**Parameters**

`vlan_id`

VLAN identifier.

`statistics`

Displays VLAN extended counters.

`brief`

Displays VLAN information in table format.

`wide`

Displays full VLAN name.

`detail`

Displays VLAN information in a detailed format.

`ethernet slot/port`

Port configured in the VLAN.

`tvf-lag-lb`

Displays transparent VLAN flooding load balancing information

`detail`

Displays transparent VLAN flooding load balancing information in detail.

**Modes**

Privileged EXEC mode.
Examples

The following example displays transparent VLAN flooding LAG load balancing information.

device# show vlan tvf-lag-lb
****TVF LAG Load Balancing****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 2048, Max FID groups: 512, FID group size: 4
TVF LAG Load balancing groups:
VLAN: 100, group ID: 257, FID base: 0x9800, FID count: 4
VLAN: 200, group ID: 258, FID base: 0x9804, FID count: 4
2TVF LAG Load balancing groups are configured

The following example displays the full VLAN name and information in table format.

device# show vlan brief wide

Configured PORT-VLAN entries: 16
Maximum PORT-VLAN entries: 512
Default PORT-VLAN id: 1

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT-VLAN</td>
<td>Untagged Ports: ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>100</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 4/1 to 4/8 Untagged Ports: ethe 3/1 to 3/24</td>
</tr>
<tr>
<td>200</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 3/1 to 3/24 ethe 4/1 to 4/8 Untagged Ports: ethe 1/1 to 1/2</td>
</tr>
<tr>
<td>300</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>400</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>500</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>600</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>700</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>800</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>900</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>1000</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>2000</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>3000</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>4000</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>4090</td>
<td>[None]</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
<tr>
<td>4095</td>
<td>CONTROL-VLAN</td>
<td>Statically tagged Ports: ethe 1/1 to 1/2 ethe 3/1 to 3/24 ethe 4/1 to 4/8</td>
</tr>
</tbody>
</table>

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command is modified to include the tvf-lag-lb parameter.</td>
</tr>
<tr>
<td>5.8.00</td>
<td>This command is modified to include the brief wide parameter.</td>
</tr>
</tbody>
</table>
show vlan tvf-lag-lb

Displays transparent VLAN flooding LAG load balancing information.

Syntax

show vlan tvf-lag-lb detail

Parameters

detail

Specifies the detailed VLAN flooding LAG load balancing information in the output.

Modes

Privileged EXEC mode

Usage Guidelines

The show vlan tvf-lag-lb command displays transparent VLAN flooding LAG load balancing information.

Examples

The following example displays transparent VLAN flooding LAG load balancing information:

device#show vlan tvf-lag-lb
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 1024, FID group size: 4
2 TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done

The following example displays the detailed transparent VLAN flooding LAG load balancing information:

device#show vlan tvf-lag-lb detail
**** TVF LAG Load Balancing ****
TVF LAG Load Balancing is enabled!
TVF FID pool size: 4096, Max FID groups: 1024, FID group size: 4
2 TVF LAG Load balancing groups are configured
TVF LAG Load balancing FID programming is done

TVF LAG Load balancing groups:
VLAN: 100, group ID: 33, FID base: 0x9ffe, FID count: 4
VLAN: 200, group ID: 34, FID base: 0x9ff8, FID count: 4

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to include additional information in the command output.</td>
</tr>
</tbody>
</table>
Commands Si - Z

slow-start

Configures a slow-start timer interval to extend the time interval beyond the dead-interval time before a Virtual Router Redundancy Protocol Extended (VRRP-E) master device assumes the role of master device after being offline. When the original master device went offline, a backup VRRP-E device with a lower priority became the master device.

Syntax

slow-start seconds [ use-track-port [ restart ] ]
no slow-start seconds [ use-track-port [ restart ] ]

Command Default

If a slow-start timer is not configured, the master device assumes control from a backup device immediately after the dead interval.

Parameters

seconds
Sets the number of seconds for the slow-start timer. Range from 1 through 57600.

use-track-port
Implements a slow-start timer for the first tracked port "up" state change, in addition to the VRRP-E initialization state.

restart
Restarts the slow-start timer for subsequent tracked port "up" state changes after the initial tracked port state change.

Modes

VRRP-E router configuration mode

Usage Guidelines

When the VRRP-E slow-start timer is enabled, if the master VRRP-E device goes down, the backup device with the highest priority takes over after the expiration of the dead interval. If the original master device subsequently comes back up again, the amount of time specified by the VRRP-E slow-start timer elapses before the original master device takes over from the backup device (which became the master device when the original master device went offline).

The slow-start allows for protocol convergence and can also be used for tracked port state changes. If the use-track-port option is not configured, the slow-start timer will be started only for the VRRP-E master device initialization, not for any tracked port state change.

This command is supported only for VRRP-E.

The no form removes the slow-start configuration.
Examples

The following example sets the slow-start timer interval to 30 seconds and configures the slow-start timer to run when a tracked port changes state.

device# configure terminal
device(config)# router vrrp-extended
device(config-vrrpe-router)# slow-start 30 use-track-port restart
**snmp-server community**

Configures the SNMP community string and access privileges.

**Syntax**

```plaintext
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. The default SNMP community name (string) on a device is “public” with the read-only privilege.

- `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 “public” community name 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 “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(config)# access-list 25 deny host 10.157.22.98 log
device(config)# access-list 25 deny 10.157.23.0 0.0.0.255 log
device(config)# access-list 25 deny 10.157.24.0 0.0.0.255 log
device(config)# access-list 25 permit any
device(config)# access-list 30 deny 10.157.25.0 0.0.0.255 log
device(config)# access-list 30 deny 10.157.26.0/24 log
device(config)# access-list 30 permit any
device(config)# snmp-server community public ro 25
device(config)# snmp-server community private rw 30
device(config)# write memory
```

The following example associates a view to the members of a community string.

```
device# configure terminal
device(config)# snmp-server community private rw view view1
```

The following example configures a read-only access and a read/write access for the same SNMP community. The output from the `show running-config` command shows that only one access type, the highest access level, is saved in the running configuration.

```
device# configure terminal
device(config)# snmp-server community private ro
device(config)# snmp-server community private rw
device(config)# exit
device# show running-config | inc snmp
snmp-server
snmp-server community private rw
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to allow setting just one access type for an SNMP community.</td>
</tr>
</tbody>
</table>
snmp-server context

Creates SNMP context and maps the context name to the name of a VPN routing and forwarding (VRF) instance.

Syntax

```
  snmp-server context context-name vrf vrf-name
  no snmp-server-context context-name vrf vrf-name
```

Parameters

- **context**
  
  Enables the specification of a variable `context_name` that can be passed in the SNMP PDU.

- **context_name**
  
  SNMP context name.

- **vrf**
  
  Enables the specification of a variable `vrf_name` that can be retrieved when an SNMP request is sent with the configured `context_name`.

- **vrf_name**
  
  VRF instance name.

Modes

- Global configuration mode

Usage Guidelines

The context-to-VRF mapping is one-to-one and is applicable to all SNMP versions.

Examples

The following `snmp-server context` command maps the context name “mycontext” to the VRF name “myvrf”:

```
switch(config)# snmp-server context mycontext vrf myvrf
```

The following `snmp-server context` command deletes the SNMP context to VRF map.

```
switch(config)# no snmp-server context mycontext vrf myvrf
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
snmp-server enable mib

Enables MIB support for SNMP server.

Syntax

```
snmp-server enable mib snmp-community-mib
no snmp-server enable mib snmp-community-mib
```

Command Default

MIB support is disabled by default.

Parameters

```
snmp-community-mib
```

Enables access for the SNMP community MIBs.

Modes

Global configuration mode

Usage Guidelines

The `no` form of the command disables access for SNMP-COMMUNITY-MIB.

Examples

The following example enables the snmpCommunityTable MIB support.

```
device(config)# snmp-server enable mib snmp-community-mib
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**snmp-server enable traps**

Configures error trap generation for IPsec and IKEv2.

**Syntax**

```
snmp-server enable traps [ ipsec ] [ ikev2 ]
no snmp-server enable traps [ ipsec ] [ ikev2 ]
```

**Command Default**

By default, IPsec and IKEv2 traps are enabled.

**Parameters**

- `ipsec`  
  Configures error trap generation for IPsec.

- `ikev2`  
  Configures error trap generation for IKEv2.

**Modes**

Privileged Exec mode

**Usage Guidelines**

The `no` form of this command disables the generation of IPsec and IKEv2 error traps.

**Examples**

The following example disables error trap generation for IPsec and IKEv2.

```
device# no snmp-server enable traps ipsec ikev2
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**snmp-server enable traps bum-rl-traps**

Configures the SNMP rate-limiting traps for BUM traffic on SNMP servers.

```
  snmp-server enable traps bum-rl-traps
  no snmp-server enable traps bum-rl-traps
```

**Command Default**

By default, SNMP rate-limiting traps for BUM traffic on SNMP servers are enabled.

**Modes**

**Usage Guidelines**

no

**Examples**

The following example shows how to disable SNMP rate-limiting traps for BUM traffic.

```
  device# configure terminal
  device(config)# no snmp-server enable traps bum-rl-traps
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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 group { host-ipaddr | ipv6 host-ipv6-addr } [ version v3 { auth | noauth | priv } name [ port port-num ] ]
no snmp-server group { host-ipaddr | ipv6 host-ipv6-addr } [ version v3 { auth | noauth | priv } name [ port port-num ] ]
```

Command Default

The SNMP trap receiver is not configured.

Parameters

- **host-ipaddr**
  Specifies the IP address of the trap receiver.

- **ipv6 host-ipv6-addr**
  Specifies the IPv6 address of the trap receiver.

- **version**
  Configures the SNMP version or security model.

- **v1**
  Specifies SNMP version 1.

- **v2c**
  Specifies SNMP version 2c.

- **community-string**
  Specifies an SNMP community string configured on the device.

- **v3**
  Specifies SNMP version 3.

- **auth**
  Specifies that only authenticated packets with no privacy are allowed to access the specified view. This parameter is available only for SNMPv3 user groups.

- **noauth**
  Specifies that no authentication and no privacy are required to access the specified view. This parameter is available only for SNMPv3 user groups.

- **priv**
  Specifies that authentication and privacy are required from the users to access the view. This parameter is available only for SNMPv3 user groups.
name
   Specifies the SNMP security name or user.

port port-num
   Configures the UDP port to be used by the trap receiver. The default port number is 162.

Modes
   Global configuration mode

Usage Guidelines
   The device sends all the SNMP traps to the specified hosts and includes the specified community string. Administrators can therefore filter for traps from a Brocade device based on IP address or community string. When you add a trap receiver, the software automatically encrypts the community string you associate with the receiver when the string is displayed by the CLI or Web Management interface. The software does not encrypt the string in the SNMP traps sent to the receiver.

   The SNMP community string configured can be a read-only string or a read-write string. The string is not used to authenticate access to the trap host but is instead a useful method for filtering traps on the host. For example, if you configure each of your Brocade devices that use the trap host to send a different community string, you can easily distinguish among the traps from different devices based on the community strings.

   The Multiple SNMP Community Names feature introduced the ability to configure one default community string (where a community string is not mapped to any SNMP context) and one community string per SNMP context for a single trap host. One community name per line is allowed. For protocol-specific MIBS, Brocade devices send the trap originating from specific VRF instance and the corresponding community name mapped to the SNMP context associated with that VRF is sent in the trap. When the Brocade devices send the trap originating from a default VRF instance, the default community string is sent in the trap. Using the community string in the trap, administrators can easily distinguish among the traps originated from different VRF instances. if you enter the show running-config command it displays multiple snmp-server host command instances for each host; one community name per line.

   Specifying the port allows you to configure several trap receivers in a system. With this parameter, a network management application can coexist in the same system. Devices can be configured to send copies of traps to more than one network management application.

   The no form of the command removes the configured SNMP server host.

Examples
   The following example configures 10.10.10.1 as the trap receiver.

   device(config)# snmp-server host 10.10.10.1 version v2c mypublic port 200

   The following example configures 2002::2:2 as the trap receiver and specifies that only authenticated packets with no privacy are allowed to access the specified view.

   device(config)# snmp-server host ipv6 2002::2:2 version v3 auth user-private port 110

   The following example configures multiple SNMP community names for a single trap host.

   device(config)# snmp-server host 192.168.2.1 version v1 user-community1
   device(config)# snmp-server host 192.168.2.1 version v1 user-community2
   device(config)# snmp-server host 192.168.2.1 version v1 user-community3
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to allow multiple SNMP community names to be configured for a single trap host.</td>
</tr>
</tbody>
</table>
**snmp-server mib community-map**

Maps an existing SNMP community string with an existing SNMP context.

**Syntax**

```
snmp-server mib community-map community_name context context_name
no snmp-server mib community-map community_name context context_name
```

**Parameters**

- **community-map**
  Maps SNMP community string to any routing instance specified in the variable `community_name`.

- **community_name**
  The existing or already configured SNMP community string.

- **context**
  Enables the specification of a variable `context_name` that can be passed in the SNMP PDU.

- **context_name**
  The existing or already configured SNMP context name.

**Modes**

Global configuration mode

**Usage Guidelines**

The SNMP community and SNMP context must be configured before mapping.

**Examples**

The following example enables the `snmpCommunityTable` MIB support.

```
device(config)# snmp-server mib community-map <community-name>
context <context-name>
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
spanning-tree pvst-protect

Enables or disables Per VLAN Spanning Tree (PVST) protection for all global interfaces running xSTP.

Syntax

spanning-tree pvst-protect do-disable
spanning-tree pvst-protect re-enable [ ethernet slot/port [ to slot/port ] ]
no spanning-tree pvst-protect do-disable
no spanning-tree pvst-protect re-enable [ ethernet slot/port [ to slot/port ] ]

Command Default

By default, PVST protect configuration is independent of spanning tree global configuration.

Parameters

do-disable
   Disables the PVST protection globally on VLANs when xSTP is configured and also can coexist with per VLAN xSTP configuration.

re-enable
   Re-enables the PVST protect disabled interfaces globally.

ethernet slot/port to slot/port
   Specifies an Ethernet interface or a range of Ethernet interfaces on which PVST protection is re-enabled.

Modes

Global configuration mode

Usage Guidelines

PVST is a Cisco proprietary protocol that allows a Cisco device to have multiple spanning trees. The Cisco device can interoperate with spanning trees on other PVST devices but cannot interoperate with IEEE 802.1Q devices. An IEEE 802.1Q device has all its ports running a single spanning tree. PVST+ is an extension of PVST that allows a Cisco device to also interoperate with devices that are running a single spanning tree (IEEE 802.1Q).

Brocade supports PVST plus (PVST+) by allowing a Brocade device to run multiple spanning trees (MSTP) while also interopering with IEEE 802.1Q devices. Ports automatically detect PVST+ BPDUs and enable support for the BPDUs once detected. The PVST+ support allows a Brocade device to interoperate with PVST spanning trees and the IEEE 802.1Q spanning tree at the same time.

The no spanning-tree pvst-protect do-disable command disables the PVST protect feature configuration globally, and enables all the ports which were disabled by this feature.

The no spanning-tree pvst-protect re-enable command reenables the PVST protect feature configuration globally, or for a specific or range of Ethernet interfaces and enables the specified ports.
NOTE
PVST protect configuration is not applicable for an Inter-Chassis Link (ICL) port.

Examples
The following example disables the PVST protect feature configuration globally.

```
device# configure terminal
device(config)# spanning-tree pvst-protect do-disable
```

The following example re-enables the PVST protect feature configuration on Ethernet interfaces 1/5 through 1/7

```
device# configure terminal
device(config)# spanning-tree pvst-protect re-enable ethernet 1/5 to 1/7
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
state-name

Configures the state name where the Public Key Infrastructure (PKI) entity resides.

Syntax

state-name string

no state-name string

Command Default

No state is recorded, by default.

Parameters

string

Specifies the name of the state for PKI entity.

Modes

PKI entity configuration mode

Examples

The following example configures California as the state where the PKI entity named as Brocade-entity resides.

device# configure terminal
device(config)# pki entity brocade-entity
device(config-pki-entity-brocade-entity)# state-name California

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
static-lsp

Creates a new static label-switched path (LSP) at the transit router or enters into the mode of an existing static transit LSP to modify its parameters and enable or disable the static transit LSP.

Syntax

static-lsp transit name
no static-lsp transit name

Parameters

transit name

Configures a new static LSP at a transit router. If the name is an existing static transit LSP name, it enters into the configuration mode for that static transit LSP.

Modes

MPLS configuration mode

Usage Guidelines

The LSP name must be unique within that router for static transit LSPs.

Use the no option to delete the static LSP.

Examples

The following example configures a static transit LSP named t1.

device# configure terminal
device(config)# router mpls
device(config-mpls)# static-lsp transit t1
device(config-mpls-static-transit-lsp-t1)# in-label 16
device(config-mpls-static-transit-lsp-t1)# next-hop 3.3.3.3
device(config-mpls-static-transit-lsp-t1)# out-label 17
device(config-mpls-static-transit-lsp-t1)# enable

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
static-mac-address

Configures the static MAC address on the VPLS endpoints.

static-mac-address { mac-addr ethernet slot/port }
no static-mac-address { mac-addr ethernet slot/port }

Parameters

mac_addr
Identifies the selected MAC address.

ethernet
Selects the Ethernet MAC address.

slot/port
Ethernet port of the VPLS endpoint.

Modes

Usage Guidelines

no

Multicast, broadcast, and zero-MACs cannot be configured.

Examples

The following example displays how to configure static MAC address on VPLS endpoints.

device(config)# router mpls
device(config-mpls)# vpls vpls-1 1
device(config-mpls-vpls-1)# vlan 900 inner-vlan 800
device(config-mpls-vpls-1-vlan-900)# static-mac-address 0000.1111.3333 ethernet 1/20

The following example displays removing a configured static MAC from a tagged/untagged endpoint.

device# configure terminal
device(config)# router mpls
device(config-mpls)# vpls vpls-1 1
device(config-mpls-vpls-1)# vlan 900
device(config-mpls-vpls-1-vlan-900)# no static-mac-address 0000.1111.2222 ethernet 1/23

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
**statistics-load-interval**

Configures the load interval parameter for calculating the bit rate and packet count for the access-list accounting statistics.

**Syntax**

```
statistics-load-interval { seconds | accumulated }
no statistics-load-interval { seconds | accumulated }
```

**Parameters**

*seconds*

Specifies the load interval values. Permitted values are 1, 60, or 300.

*accumulated*

Displays accumulated ACL statistics packets and bit rate counts.

**Modes**

ACL-policy sub-configuration mode

**Usage Guidelines**

The no form of the command removes the configuration of the load interval parameters for calculating the bit rate and packet count for the access-list accounting statistics.

Use the configured load interval value to display the bit rate and packet rate statistics. If the load interval is not configured, statistics of all three intervals 1s/60s/300s and accumulated statistics display.

This configuration is stored in the configuration file.

**NOTE**

This configuration applies only to policy-based routing ACLs.

**Examples**

The following example uses the load interval option to choose any one of the intervals for statistics display.

```
device(config)# acl-policy
device(config-acl-policy)# statistics-load-interval 60
device(config-acl-policy)# show access-list accounting brief policy-based-routing
```

<table>
<thead>
<tr>
<th>Intf</th>
<th>ACL</th>
<th>BitRate</th>
<th>HitRate</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/1</td>
<td>100</td>
<td>2697753600</td>
<td>2634525 (1m)</td>
</tr>
<tr>
<td>3/3</td>
<td>102</td>
<td>0</td>
<td>0 (1m)</td>
</tr>
</tbody>
</table>

The following example shows uses the non-zero statistics option.

```
device(config)# acl-policy
device(config-acl-policy)#
device(config-acl-policy)# show access-list accounting brief policy-based-routing omit-zero
```

<table>
<thead>
<tr>
<th>Intf</th>
<th>ACL</th>
<th>BitRate</th>
<th>HitRate</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/1</td>
<td>100</td>
<td>2697753600</td>
<td>2634525 (1m)</td>
</tr>
<tr>
<td>3/3</td>
<td>101</td>
<td>5210585952</td>
<td>4934267 (1m)</td>
</tr>
</tbody>
</table>
### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
subject-alt-name
Configures the alternative subject name for the Public Key Infrastructure (PKI) entity.

Syntax
subject-alt-name string
no subject-alt-name string

Parameters
string
Specifies the alternate name of the subject for the PKI entity.

Modes
PKI entity configuration mode

Usage Guidelines
If the IKE peer uses an ID other than the distinguished name (DN), then that should be mentioned in the subject-alt-name. If the certificate does not have subject-alt-name then use DN for the IKE ID.

Examples
The following example configures the alternate name of the subject for the PKI entity.

device(config)# pki entity brocade
device(config-pki-entity-brocade)# subject-alt-name red

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
summary-address (OSPFv3)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address IPv6-addr/mask

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A:B:C:D/LEN

IPv6 address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified IPv6 address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

You can configure up to 32 address ranges.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.

If you use redistribution filters in addition to address ranges, the Brocade device applies the redistribution filters to routes first, then applies them to the address ranges.

If you disable redistribution, all the aggregate routes are flushed, along with other imported routes.

This option affects only imported, type 5 external routes. A single type 5 LSA is generated and flooded throughout the AS for multiple external routes.
Examples

The following example configures a summary address of 2001:db8::/24 for routes redistributed into OSPFv3.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# summary-address 2001:db8::/24

NOTE
In this example, the summary prefix 2001:db8::/24 includes addresses 2001:db8::/1 through 2001:db8::/24. Only the address 2001:db8::/24 is advertised in an external link-state advertisement.
**suppress-acl-seq**

Hides or suppresses the display and storage of sequence numbers for ACL entries.

**Syntax**

```
suppress-acl-seq
no suppress-acl-seq
```

**Modes**

acl-policy configuration mode

**Usage Guidelines**

Use this command if you need to downgrade a device to an earlier version of software that does not support ACL entry sequence numbers, you should configure `suppress-acl-seq` prior to the downgrade. Otherwise, ACL configurations created with the `suppress-acl-seq` parameter will result in an error on previous releases.

The `no` version of this command resets the configuration to display sequence numbers.

**Examples**

The following example suppresses ACL entry sequence numbering:

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# suppress-acl-seq
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**suppress-ipv6-priority-mapping**

Suppresses the IPv6-priority-mapping command from IPv6 filters. This command is only to be used before starting the downgrade process.

**Syntax**

```
suppress-ipv6-priority-mapping
```

**Modes**

```
acl-policy
```

**Usage Guidelines**

Use this command if you need to downgrade a device to an earlier version of software that does not support ACL ipv6-priority-mapping, you should configure **suppress-ipv6-priority-mapping** prior to the downgrade. Otherwise, ACL configurations created with the **ipv6-priority-mapping** parameter will result in an error on previous releases.

To reset the **ipv6-priority-mapping**, re-apply the command using the **ipv6-access-list**.

**Examples**

The following example suppresses ACL IPv6 priority-mapping.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# suppress-ipv6-priority-mapping
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon fe link auto-tune

Enables auto tuning on the fabric element (FE).

Syntax

- `sysmon fe link auto-tune`
- `no sysmon fe link auto-tune`

Command Default

Auto tuning on the FE is enabled by default.

Modes

- Global configuration mode

Usage Guidelines

The `no` form of the command disables auto-tuning on the FE.

Examples

The following example disables auto-tuning on the FE.

```
device(config)# no sysmon fe link auto-tune
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

sysmon ipc rel-q-mon enable

Enables LP and MP IPC reliable transmission (TX) queue monitoring and the generation of syslog messages when the IPC reliable TX queue is stuck or recovers from being stuck.

Syntax

sysmon ipc rel-q-mon enable
no sysmon ipc rel-q-mon enable

Command Default

IPC reliable TX queue monitoring is disabled.

Modes

Global configuration mode

Usage Guidelines

The no form of the command disables LP and MP IPC reliable transmission (TX) queue monitoring.

Examples

The following example enables IPC reliable TX queue monitoring and syslog message generation.

device(config)# sysmon ipc rel-q-mon enable

The following example disables IPC reliable TX queue monitoring and syslog message generation.

device(config)# no sysmon ipc rel-q-mon enable

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon lp-high-cpu enable

Configures high cpu-usage and reporting on interface modules.

Syntax

sysmon lp-high-cpu enable [ all | slot-number ]
no sysmon lp-high-cpu enable [ all | slot-number ]

Parameters

all
  Specifies CPUs on all slots to be monitored.

slot-number
  Specifies the slot number for the CPU to be monitored.

Modes

Privileged EXEC configuration mode.

Usage Guidelines

Use this command to set up the monitoring on one or all LP CPUs.

The no form of this command disables the LP CPU high-usage monitoring.

Examples

The following example enables monitoring on all CPUs.

device(config)# sysmon lp-high-cpu enable all

The following example enables monitoring on the CPU in slot 7.

device(config)# sysmon lp-high-cpu enable 7

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon lp-high-cpu threshold

Configures high cpu-usage and reporting on interface modules.

Syntax

```
sysmon lp-high-cpu threshold decimal-percent-number

no sysmon lp-high-cpu threshold
```

Parameters

- **decimal-percent-number**
  Specifies the usage threshold for all CPUs to be monitored. Acceptable range of values is from 50 to 100 with 80 as the default value.

Modes

Privileged EXEC configuration mode.

Usage Guidelines

Use this command to set up the usage threshold for collecting data on the monitored LP CPUs. The default CPU threshold is 80% unless explicitly specified. The set threshold applies to all LP(s).

The no form of this command resets the usage threshold to 80% for all CPUs.

Examples

The following example sets the usage threshold to 90% for all monitored CPUs.

```
device(config)# sysmon lp-high-cpu threshold 90
```

The following resets the usage threshold to 80% for all monitored CPUs.

```
device(config)# no sysmon lp-high-cpu threshold
```

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**sysmon mp-high-cpu cpu-threshold**

Configures the MP CPU usage threshold that triggers data collection into a log file.

**Syntax**

```plaintext
sysmon mp-high-cpu cpu-threshold decimal-cpu-percentage
no sysmon mp-high-cpu cpu-threshold
```

**Command Default**

When high CPU monitoring on the MP is enabled, the default CPU usage threshold is 90 percent.

**Parameters**

`decimal-cpu-percentage`

Specifies the threshold based on the percentage of usage on the monitored MP CPUs. The percentage values are from 60 through 100. The default percentage value is 90.

**Modes**

Global configuration mode

**Usage Guidelines**

Use this command to configure the usage threshold for collecting data on the monitored active and standby MP CPUs when MP CPU high-usage monitoring is enabled.

The threshold is based on the percentage of CPU usage on the active or standby MP.

The `no` form of the command resets the usage threshold to the default value of 90 percent for the MP CPUs.

**Examples**

The following command example sets the usage threshold to 70 percent for the MP CPUs.

```plaintext
device(config)# sysmon mp-high-cpu cpu-threshold 70
```

The following command example resets the usage threshold to 90 percent for the MP CPUs.

```plaintext
device(config)# no sysmon mp-high-cpu cpu-threshold
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**sysmon mp-high-cpu enable**

Enables MP CPU high-usage monitoring and data collection in a log file.

**Syntax**

```plaintext
sysmon mp-high-cpu enable
no sysmon mp-high-cpu enable
```

**Command Default**

MP CPU high-usage monitoring is disabled.

**Modes**

Global configuration mode

**Usage Guidelines**

Use this command to enable CPU high-usage monitoring on the active and standby MP CPUs and log high CPU usage events in a log file. Monitoring is enabled when the MP is in the up state.

The `no` form of the command disables MP CPU high-usage monitoring and data collection. Also, the threshold settings that were configured when monitoring was enabled are reset to their default values of 90 percent and 400 ms.

**Examples**

The following example enables MP CPU high-usage monitoring and data collection.

```plaintext
device(config)# sysmon mp-high-cpu enable
```

The following example disables MP CPU high-usage monitoring and data collection. Also, the threshold settings are reset to their default values.

```plaintext
device(config)# no sysmon mp-high-cpu enable
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon mp-high-cpu task-threshold

Configures the MP CPU task threshold that triggers data collection in a log file.

Syntax

```
sysmon mp-high-cpu task-threshold ms
no sysmon mp-high-cpu task-threshold
```

Command Default

When high CPU monitoring on the MP is enabled, the default task threshold is 400 milliseconds (ms).

Parameters

```
ms
```

Specifies the threshold based on the time in milliseconds that the task holds the MP CPU. The millisecond values are from 100 through 500. The default threshold is 400.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the task threshold for collecting data on the monitored active and standby MP CPUs when MP CPU high-usage monitoring is enabled.

The threshold is the amount of time that the task holds the MP CPU.

The no form of the command resets the task threshold to the default value of 400 ms.

Examples

The following example sets the task threshold to 200 ms.

```
device(config)# sysmon mp-high-cpu task-threshold 200
```

The following example resets the task threshold to 400 ms.

```
device(config)# no sysmon mp-high-cpu task-threshold
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon np memory-errors
Configures memory error monitoring and reporting on interface modules.

Syntax

sysmon np memory-errors [ action { none | syslog | syslog-and-trap | trap } ]
sysmon np memory-errors [ polling-period secs ]
sysmon np memory-errors [ schedule { after dd:hh:mm | at hh:mm:ss mm-dd-yy | now } runs ]
sysmon np memory-errors [ slot { all | slot } ]

no sysmon np memory-errors [ action { none | syslog | syslog-and-trap | trap } ]
no sysmon np memory-errors [ polling-period secs ]
no sysmon np memory-errors [ schedule { after dd:hh:mm | at hh:mm:ss mm-dd-yy | now } runs ]
no sysmon np memory-errors [ slot { all | slot } ]

Parameters

action
Specifies the action taken when NP memory errors are detected. The default action is syslog-and-trap.

none
No action; reporting of errors is disabled. In the no form of the command, specifying the action as none restores the default action (syslog-and-trap).

tsyslog
Generates a syslog message.

syslog-and-trap
Generates a syslog message and an SNMP trap.

trap
Sends an SNMP trap.

polling-period secs
Specifies the frequency of polling for NP memory errors. The range is from 1 through 65535. The default value is 60 seconds.

schedule
Configures the test scheduling.

after dd:hh:mm
Specifies that the test is run after the specified amount of time.

at hh:mm:ss mm-dd-yy
Specifies that the test is run at the specified time and date.

now
Specifies that the test is run immediately. This is defined as on-demand testing.

runs
Specifies the number of test runs.

**slot**

Specifies the slots on which the test is run.

**all**

Specifies that the test is run on all slots.

**slot**

Specifies the slot number on which the test is to be run. You can specify up to 8 slot numbers.

### Modes

Global configuration mode

### Usage Guidelines

The **action** parameter controls the generation of syslog messages or SNMP traps. These messages cannot be controlled by the **no snmp-server enable traps** command or the **no logging enable** command. If the **action** option is configured as **syslog** followed by a configuration of the **trap** action, the action becomes **syslog-and-trap**.

The **polling-period** parameter determines the interval between checks for NP memory errors. Reporting may not happen within the polling interval; it may be delayed by factors such as a high CPU load on either the interface or management modules, low memory, or other factors.

Memory errors are detected on the interface module. Errors may not be reported if there is a communication problem between the management module and the interface module.

The **no** form of this command disables memory error monitoring on interface modules.

### Examples

The following example specifies polling for NP memory errors at 10 second intervals.

```
device# configure terminal
device(config)# sysmon np memory-errors polling-period 10
```

The following example disables reporting of NP memory errors.

```
device# configure terminal
device(config)# sysmon np memory-errors action none
```

The following example disables monitoring of memory errors on interface modules.

```
device# configure terminal
device(config)# no sysmon np memory-errors
```

The **no** form of the command specifying a **polling-period** value restores the default polling interval. For example, the following example restores the polling interval to the default value of 60 seconds.

```
device# configure terminal
device(config)# no sysmon np memory-errors polling-period 1000
```

The following example removes the **syslog** action.

```
device# configure terminal
device(config)# no sysmon np memory-errors action syslog
```
The following example restores the default action of `syslog-and-trap`. The `no` form of the command specifying the `action none` parameters restores the default action.

device# configure terminal
device(config)# no sysmon np memory-errors action none

### History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon port port-crc-test
Enables the port CRC error monitoring test.

Syntax

sysmon port port-crc-test [ action {none | port-disable | syslog } ]
sysmon port port-crc-test [ counter port-crc-counter less-than crc-count ]
sysmon port port-crc-test [ log-backoff num ]
sysmon port port-crc-test [ polling-period seconds ]
sysmon port port-crc-test [ schedule { after dd:hh:mm runs | at hh:mm:ss mm-dd-yy runs | now } ]
sysmon port port-crc-test [ slot { all | slot } ]
sysmon port port-crc-test [ threshold num-failures num-polls ]
no sysmon port port-crc-test [ action {none | port-disable | syslog } ]
no sysmon port port-crc-test [ counter port-crc-counter less-than crc-count ]
no sysmon port port-crc-test [ log-backoff num ]
no sysmon port port-crc-test [ polling-period seconds ]
no sysmon port port-crc-test [ schedule { after dd:hh:mm runs | at hh:mm:ss mm-dd-yy runs | now } ]
no sysmon port port-crc-test [ slot { all | slot } ]
no sysmon port port-crc-test [ threshold num-failures num-polls ]

Parameters

action
   Specifies a sysmon action configuration.
   none   No action.
   port-disable   Disable port.
   syslog   Generates a syslog message.

counter port-crc-counter less-than crc-count
   Specifies the port CRC error count limit for the configured polling period. The range of values is 0 through 65535.
   The default value is 20.

polling-period secs
   Specifies the polling period in seconds. The range of values is 0 through 65535. The default value is 60 seconds.

schedule
   Specifies the schedule of the test.
   after dd:hh:mm runs
Specifies that the test is run after the specified amount of time and for the number of test runs.

at hh:mm:ss mm-dd-yy runs
Specifies that the test is run at the specified time and date and for the number of test runs.

now
Specifies that the test is run immediately. This is defined as on-demand testing.

slot
Specifies the slots on which the test is run.

all
Specifies that the test is run on all slots.

slot
Specifies the slot number on which the test is to be run. You can specify up to 8 slot numbers.

threshold
Specifies the threshold of the diagnostic test.

num-failures
Specifies the number of failed test runs. The range of values is 1 through 31.

num-polls
Specifies the number of polls (tests). The range of values is 2 through 31.

Modes
Global configuration mode

Usage Guidelines
The no form of this command disables the port CRC error monitoring test.

Examples
The following example disables the port CRC error monitoring test.

device(config)# no sysmon port port-crc-test

The following example sets the diagnostic action to disable the port when the port CRC error limit crosses the configured threshold.

device(config)# sysmon port port-crc-test action port-disable

The following example configures the port CRC error counter limit to 20.

device(config)# sysmon port port-crc-test counter port-crc-counter less-than 20

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon sfm walk auto

Enables an option that automatically triggers a high-speed Switch Fabric Module (hSFM) walk automatically upon reaching a configured threshold.

Syntax

```
sysmon sfm walk auto
no sysmon sfm walk auto
```

Command Default

The command is disabled by default.

Modes

Global configuration mode

Usage Guidelines

**NOTE**

Auto-tuning and hSFM auto-walk cannot operate at the same time. To avoid conflict, configure auto-tuning and hSFM auto-walk to trigger consecutively. Whichever triggers first runs, after which the other one runs.

The **no** form of this command disables the automatic triggering of `sysmon sfm walk auto`.

Examples

The following example enables `sysmon sfm walk auto`.

```
device# configure terminal
device(config)# sysmon sfm walk auto
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00b</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
sysmon sfm walk polling-period

Configuring a polling period for re-assembly errors located on a high-speed Switch Fabric Module (hSFM).

Syntax

```
sysmon sfm walk polling-period value
```

Command Default

The command is disabled by default.

Parameters

```
value
```

Sets the polling period in a range from 1 to 600 seconds. The default setting is 30 seconds.

Modes

Global configuration mode

Usage Guidelines

Use this command to set the interval between polling periods for re-assembly errors.

Examples

The following example configures the sfm walk polling-period to be 50 seconds.

```
device# configure terminal
device(config)# sysmon sfm walk polling-period 50
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00b</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon sfm walk redundancy-check
Setting an option to automatically trigger an SFM redundancy check during a high-speed Switch Fabric Module (hSFM) walk.

Syntax
- `sysmon sfm walk redundancy-check`
- `no sysmon sfm walk redundancy-check`

Command Default
The redundancy check option is enabled.

Modes
- Global configuration mode

Usage Guidelines
For an SFM walk to begin, a redundant SFM is required. The no form of this command will trigger auto hsfm walk if N+1 SFMs are unavailable.

Examples
The following example enables a `sysmon sfm walk redundancy-check`

```
device# configure terminal
device(config)# sysmon sfm walk redundancy-check
```

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00b</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
sysmon sfm walk start

Enables a manual high-speed Switch Fabric Module (hSFM) walk.

Syntax

sysmon sfm walk start

Command Default

By default, sysmon sfm walks are automatically triggered.

Modes

Global configuration mode.

Usage Guidelines

Use this command to manually start a sysmon sfm walk.

NOTE

Auto-tuning and hSFM walk cannot operate at the same time. To avoid conflict, auto-tuning and hSFM walk will be performed consecutively. Whichever is triggered first will run and then the other will be performed.

Examples

The following example manually enables sysmon sfm walk.

device# configure terminal
device(config)# sysmon sfm walk start

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00b</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon sfm walk status
Displays the status of a high-speed Switch Fabric Module (hSFM) walk.

Syntax
sysmon sfm walk status

Command Default
This command will show the status of the current SFM walk. If the auto sfm walk is disabled, the status of the last walk will be displayed.

Modes
Global configuration mode.

Usage Guidelines
The command is used to display the current status of an active sfm walk or sfm auto-walk.

Examples
The following example enables sysmon sfm walk status.

```
device# configure terminal
device(config)# sysmon sfm walk status
```

```
SFM Walk status            : Isolated an SFM
Number of SFM walk done    : 1
Auto walk                  : Enabled
Manual walk                : Not started
Autotune in progress       : 0
Autotunes on isolated SFM  : 0
AutoWalk timers :
    Threshold for re-assembly 1, polling period 30, Counter reset time 10000
Redundancy check   : Enable
AutoWalk result :
    Isolated SFM 3, Current SFM 3 (SFM range (1-4), FE (1-3))
Re-assembly error count 0, MCAST FID updates 0
Reachability register (0x461) dump :
    SFM1/FE1: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM1/FE2: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM1/FE3: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM2/FE1: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM2/FE2: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM2/FE3: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM3/FE1: val=0x01f3f000 : 00000001-11110011-11110000-00000000b [Non-reachable, autotune 0]
    SFM3/FE2: val=0x01f3f000 : 00000001-11110011-11110000-00000000b [Non-reachable, autotune 0]
    SFM3/FE3: val=0x01f3f000 : 00000001-11110011-11110000-00000000b [Non-reachable, autotune 0]
    SFM4/FE1: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM4/FE2: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
    SFM4/FE3: val=0x01f3f009 : 00000001-11110011-11110000-00001001b [Reachable, autotune 0]
```
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.7.00b</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon sfm walk stop

Stops any currently running high-speed Switch Fabric Module (hSFM) walk.

Syntax

    sysmon sfm walk stop

Command Default

Existing fsm walks run until completed.

Modes

    Global configuration mode

Usage Guidelines

This command is used to stop a currently running walk or revert an already completed walk. For example, if an SFM walk is completed and an SFM is isolated, `sysmon sfm walk stop` will re-enable the isolated SFM. This command is effective on both manual and auto SFM walks.

Examples

The following example stops an active sysmon sfm walk.

    device# configure terminal
    device(config)# sysmon sfm walk stop

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.700b</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon sfm walk threshold

Configures the threshold value for a minimum re-assembly count to isolate an SFM during an SFM walk.

Syntax

```
system sfm walk threshold value
no system sfm walk threshold
```

Command Default

The default sysmon sfm walk threshold value is 1.

Parameters

`value`

Configures the minimum threshold value for re-assembly count range in a range from 1 to 65535. The default setting is 1.

Modes

Global configuration mode

Usage Guidelines

The no form of this command will reset the threshold value to the default.

Examples

The following example configures the `sysmon sfm walk threshold` to 5.

```
device# configure terminal
device(config)# sysmon sfm walk threshold 5
```

The following is an example of the syslog showing the resulting actions when re-assembly errors cross the configured threshold value of 5.

```
SYSLOG: <9>Oct 14 00:41:18 System: Health Monitoring: TM Egress data errors detected on LP 15/TM 1
SYSLOG: <14>Oct 14 00:41:18 System: SFM-WALK: Auto SFM walk started
SYSLOG: <9>Oct 14 00:41:32 System: Health Monitoring detects an issue on egress LP 3/TM 1
SYSLOG: <14>Oct 14 00:41:32 System: SFM-WALK: Auto SFM walk started
SYSLOG: <14>Oct 14 00:41:32 System: SFM-WALK: SFM walk in progress
SYSLOG: <9>Oct 14 00:41:46 System: Health Monitoring detects an issue on egress LP 1/TM 1
SYSLOG: <14>Oct 14 00:41:46 System: SFM-WALK: Auto SFM walk started
SYSLOG: <14>Oct 14 00:41:46 System: SFM-WALK: SFM walk in progress
SYSLOG: <9>Oct 14 00:41:48 System: Health Monitoring detects an issue on egress LP 2/TM 2
SYSLOG: <14>Oct 14 00:41:48 System: SFM-WALK: Auto SFM walk started
SYSLOG: <14>Oct 14 00:41:48 System: SFM-WALK: SFM walk in progress
SYSLOG: <9>Oct 14 00:42:01 System: SFM-WALK: Re-assembly errors (125) more than threshold (5). Move to next SFM #2.
SYSLOG: <14>Oct 14 00:42:42 System: SFM-WALK: Re-assembly errors (126) more than threshold (5). Move to next SFM #3.
SYSLOG: <14>Oct 14 00:43:22 System: SFM-WALK: Re-assembly errors (0) less than threshold (5). Isolated SFM #3.
SYSLOG: <14>Oct 14 00:43:22 System: SFM-WALK: SFM walk completed. Faulted SFM #3 and removed from service.
```
### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.700b</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
sysmon tm link auto-tune
Enables auto tuning on the traffic manager (TM).

Syntax
   sysmon tm link auto-tune
   no sysmon tm link auto-tune

Command Default
Auto tuning on the TM is enabled by default.

Modes
Global configuration mode

Usage Guidelines
The no form of the command disables auto-tuning on the TM.

Examples
The following example disables auto-tuning on the TM.

   device(config)# no sysmon tm link auto-tune

History
<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
system np control-ram-threshold

Configures the CSRAM error reporting threshold parameter for low level memory events.

Syntax

system np control-ram-threshold threshold
no system np control-ram-threshold threshold

Command Default

The default threshold value is 10.

Parameters

threshold

Specifies the configurable threshold range when low level memory events are exceeded. The decimal range is from 0 - 120 events. The default value is 10.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the CSRAM threshold parameter when monitoring low level memory events occurring with the internal data path of the network processor. This command is enabled by default. Use the no form of the command to reset the threshold value to default. Use the command to disable the monitoring of low level memory events. A syslog message and a trap is generated when the CSRAM error events recorded in the rolling window exceeds the configured threshold parameter for the specified port range.

NOTE
Configuring the CSRAM error reporting threshold parameter is supported only on the Brocade NetIron CER Series and the Brocade NetIron CES Series platforms.

Examples

The following example configures the CSRAM error reporting threshold parameter to 20 events.

device# configure terminal
device(config)#system np control-ram-threshold 20
Use the `show run` command to display the CSRAM error reporting threshold parameter to 20 events.

```bash
device(config)#show run
!
ver V5.7.0Txxx
!
!
no spanning-tree
!
!
vlan 1 name DEFAULT-VLAN
!
!
!
!
system np control-ram-threshold 20
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
system np lpm-ram-threshold

Configures the LPM memory error reporting threshold parameter for low level memory events.

Syntax

```
system np lpm-ram-threshold threshold

no system np lpm-ram-threshold threshold
```

Command Default

Configuring the LPM memory error reporting threshold parameters is enabled by default.

Parameters

`threshold`

Specifies the configurable threshold range when low level memory events are exceeded. The decimal range is from 0 - 120 events. The default value is 10.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the LPM memory threshold parameter when monitoring low level memory events occurring with the internal data path of the network processor. The command is enabled by default. Use the `no` form of the command to reset the threshold value to default. Use this command to disable the monitoring of low level memory events. A syslog message and a trap is generated when the LPM memory error events recorded in the rolling window exceeds the configured threshold parameter for the specified port range.

**NOTE**

Configuring the LPM memory error reporting threshold parameter is supported only on the Brocade NetIron CER Series and the Brocade NetIron CES Series platforms.

Examples

The following example configures the LPM memory error reporting threshold parameter to 20 events.

```
device# configure terminal
device(config)# system np lpm-ram-threshold 20
```
Use the **show run** command to display the LPM memory error reporting threshold parameter to 20 events.

```
device(config)#show run
!
ver V5.7.0Txxx
!
!
no spanning-tree
!
!
vlan 1 name DEFAULT-VLAN
!
!
!
!
!
!
!
!

system np lpm-ram-threshold 20
!
!
!
!
!
!
!
!
!
!
!
!
!
end
```

### History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.700</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**system-init**

Sets system initialization value. A reload is required before this command takes effect.

**Syntax**

```
system-init block-g1-sfm
system-init fabric-data-mode { force-normal | force-turbo }
system-init fabric-failure-detection
system-init fe-access-recovery-disable
system-init max-tm-queues num
system-init mlxe32-24x10g-enable [ max-tm-queue-4 ]
system-init tm-credit-size { credit_1024b | credit_256b }
no system-init block-g1-sfm
no system-init fabric-data-mode { force-normal | force-turbo }
no system-init fabric-failure-detection
no system-init fe-access-recovery-disable
no system-init max-tm-queues num
no system-init mlxe32-24x10g-enable [ max-tm-queue-4 ]
no system-init tm-credit-size { credit_1024b | credit_256b }
```

**Parameters**

- **block-g1-sfm**
  
  Configures the system to block the g1 switch fabric module.

- **fabric-data-mode**
  
  Configures the fabric data mode.

  - `force-normal`
    
    Forces the fabric to use normal data mode.

  - `force-turbo`
    
    Forces the fabric to use turbo data mode.

- **fabric-failure-detection**
  
  Configures the system to automatically detect and shutdown the failure fabric.

- **fe-access-recovery-disable**
  
  Disables a RAS feature that will power-cycle switch fabric module if SW cannot access fabric element.

- **max-tm-queues num**
  
  Configures the maximum number of queues in the traffic manager to 4.

- **mlxe32-24x10g-enable**
  
  Configures the system to accept 24x10G module.
max-tm-queue-4
   Configures the 4-priority mode to allow the coexistence of 24x10G and 2x10, 4x10, and 20x1 modules.

tm-credit-size
   Configures the traffic manager credit size.

credit_1024b
   Specifies a credit size of 1024 bytes.

credit_256b
   Specifies a credit size of 256 bytes.

Modes
   Global configuration mode

Usage Guidelines
   When using the fe-access-recovery-disable option, note that the system does periodic monitoring of FE access and keeps a log for this by code monitoring fabric links and kicks off when number of links down exceeds defined threshold for traffic. However if failure detection configuration is enabled, you need to use these commands for recovery.

Examples
   device# configure terminal
device(config)#system-init fe-access-recovery-disable
device(config)#exit
device# reload

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
system-max ecmp-pram-block-size

Configures the maximum parameter random-access memory (PRAM) block allocation for Equal-Cost MultiPath (ECMP) routes.

Syntax

```
system-max ecmp-pram-block-size num
no system-max ecmp-pram-block-size num
```

Parameters

`num`

Specifies the maximum PRAM block-size value. Valid values are 8, 16, and 32 (default is 32).

Modes

Global configuration mode

Usage Guidelines

The control plane (through the IP load-sharing command) supports up to 32 next hops per route. The actual number of next hops which are programmed in hardware is controlled by this command. When configuring the command to a value lesser than the value configured for IP load-sharing or IPv6 load-sharing, a warning message displays and the value is accepted. When configuring IP load-sharing or IPv6 load-sharing to a value greater than that configured for the command, a warning message displays and the value is accepted.

This command is not supported on Brocade NetIron CER Series and Brocade NetIron CES Series devices.

**NOTE**

Using this command requires a system restart in order for the new setting to take effect.

Examples

The following example sets the maximum PRAM block-size value to 16.

```
device# configure terminal
device(config)# system-max ecmp-pram-block-size 16
```

Reload required. Please write memory and then reload or power cycle the system.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.

History

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**system-max ip-arp**

Sets the ARP scaling number.

**Syntax**

```
system-max ip-arp num
```

**Parameters**

`num`

Value range is 2048 - 131072. The default value is 8192.

**Modes**

Global configuration mode

**Usage Guidelines**

Use this command to set the maximum number of ARP entries. This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured `system-max` command does not take effect during a hitless-reload.

**Examples**

The following example sets the maximum number of ARP entries at 3005.

```
device# configure terminal
device(config)# system-max ip-arp 3005
```

Reload required. Please write memory and then reload or power cycle the system. Failure to reload could cause system instability on failover. Newly configured `system-max` will not take effect during hitless-reload.

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was modified to scale up to 128K ARP entries.</td>
</tr>
</tbody>
</table>
system-max ipv6-receive-cam

Configures the number of IPv6 rACL entries in CAM. The no form of this command removes the configured limit and restores the default value.

Syntax

system-max ipv6-receive-cam num
no system-max ipv6-receive-cam num

Parameters

num

Configures the number of IPv6 rACL entries in CAM. The valid range is from 0 through 8192. The default value is 0.

Modes

Global configuration mode

Usage Guidelines

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured system-max command does not take effect during a hitless-reload.

Examples

The following example sets the number of IPv6 rACL entries in CAM to 4096.

device# configure terminal
device(config)# system-max ipv6-receive-cam 4096
Reload required. Please write memory and then reload or power cycle the system.
Failure to reload could cause system instability on failover.
Newly configured system-max will not take effect during hitless-reload.

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
system-max ipv6-vrf-route

Configures the maximum number of IPv6 routes that can be created per VRF instance.

Syntax

```
system-max ipv6-vrf-route num
no system-max ipv6-vrf-route num
```

Command Default

By default, the maximum number of IPv6 routes per VRF instance is not configured.

Parameters

```
um
```

The number of IPv6 routes that can be created per VRF instance. Valid IPv6 route values are 1024 through 131072. The default value is 8192.

Modes

Global configuration mode.

Usage Guidelines

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured `system-max` command does not take effect during a hitless-reload.

Use the `no` form of the command to reset the maximum number of IPv6 routes that was configured for a VRF instance.

Examples

The following example configures 4000 IPv6 routes per VRF instance.

```
device# configure terminal
device(config)# system-max ipv6-vrf-route 4000
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was modified.</td>
</tr>
</tbody>
</table>
**system-max ip-vrf-route**

Configures the maximum number of IPv4 routes that can be created per VRF instance.

**Syntax**

```
system-max ip-vrf-route num
no system-max ip-vrf-route num
```

**Command Default**

By default, the maximum number of IPv4 routes per VRF instance are not configured.

**Parameters**

`num`

The number of IPv4 routes that can be created per VRF instance. Valid IPv4 route values are 128 through 524288. The default value is 1024.

**Modes**

Global configuration mode.

**Usage Guidelines**

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured `system-max` command does not take effect during a hitless-reload.

Use the `no` form of the command to reset the maximum number of IPv4 routes that was configured for a VRF instance.

**Examples**

The following example configures 200 IPv4 routes per VRF instance.

```
device# configure terminal
device(config)# system-max ip-vrf-route 200
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.8.00</td>
<td>This command was modified.</td>
</tr>
</tbody>
</table>
system-max rstp

Defines the maximum number of Rapid Spanning Tree Protocol (RSTP) instances that can be configured on the Brocade NetIron XMR and MLX Series devices.

Syntax

system-max rstp number-of-instances

no system-max rstp number-of-instances

Parameters

number-of-instances

Specifies the maximum number of RSTP instances that can be configured on a Brocade device. The valid number of instances are 1 through 256. The default value is 32.

Modes

Global configuration mode

Usage Guidelines

This command is applicable to the Brocade NetIron MLX Series and Brocade NetIron XMR Series only.

Requires a reload. Failure to reload causes system instability on failover. A newly configured system-max command does not take effect during a hitless-reload.

The no form of the command removes the configured RSTP instances.

NOTE

Before you downgrade from Brocade NetIron Release 5.9 to a lower release and restart the device, it is recommended that you reduce the number of RSTP instances to 128 or a lower value using the system-max rstp command. However, if you upgrade from Brocade NetIron Release 5.8 (or previous releases) to 5.9 and restart, there is no change in the RSTP configuration or operation since the lower number of RSTP instances are anyway supported.

Examples

The following example enables configuring a maximum of 48 RSTP instances on the device.

device# configure terminal
device(config)# system-max rstp 48

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to increase the maximum valid RSTP instances from 128 to 256.</td>
</tr>
</tbody>
</table>
system-max trunk-num

Specifies the maximum number of trunks that can be set in the Brocade devices.

Syntax

\[
\text{system-max trunk-num value}
\]
\[
\text{no system-max trunk-num value}
\]

Command Default

If this command is not entered, the default number is 128.

Parameters

\[\text{value}\]

Specifies the maximum number of trunks that can be set on a Brocade device. The valid values are 32, 64, 128, and 1024. The default value is 128.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the previously specified maximum number of trunks.

**NOTE**

Using this command requires a system restart in order for the new setting to take effect.

Examples

The following example sets the maximum number of trunks to 64.

\[
\text{device# configure terminal}
\]
\[
\text{device(config)# system-max trunk-num 64}
\]

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.00a</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>
system-max tvf-lag-lb-fid-group

Configures maximum FID group size for transparent VLAN flooding LAG load balancing globally.

Syntax

```
system-max tvf-lag-lb-fid-group number
no system-max tvf-lag-lb-fid-group
```

Command Default

The default maximum FID group size is 2.

Parameters

- `number` Specifies the decimal value of the FID number defined per group. Valid values are 2, 4, 8.

Modes

- Global configuration mode

Usage Guidelines

The `system-max tvf-lag-lb-fid-group` command configures maximum FID group size for transparent VLAN flooding LAG load balancing globally. Valid values defined per group are 2, 4, 8.

**NOTE**

After configuring group size, execute the `write memory` command and restart the router. Configuring a new maximum FID group size could cause instability on failover.

Use the `no` form of this command to disable the configured max group size.

Examples

The following example configures a max group size of 4 for transparent VLAN flooding LAG load balancing:

```
device(config)# system-max tvf-lag-lb-fid-group 4
```

To disable the max group size configuration, use the following command:

```
device(config)# no system-max tvf-lag-lb-fid-group
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**system-max tvf-lag-lb-fid-pool**

Configures maximum FID pool size for transparent VLAN flooding LAG load balancing globally.

**Syntax**

```
system-max tvf-lag-lb-fid-pool number
no system-max tvf-lag-lb-fid-pool
```

**Parameters**

- `number`
  Specifies the decimal value of FID pool size defined. The valid values are 0, 512, 1024, 2048, and 4096. The default value is 0. Setting the value as 0 will disable transparent VLAN flooding LAG load balancing globally.

**Modes**

Global configuration mode

**Usage Guidelines**

Use the `no system-max tvf-lag-lb-fid-pool` command to disable the pool size configuration.

The `system-max tvf-lag-lb-fid-pool` command configures maximum pool size for transparent VLAN flooding LAG load balancing globally.

**NOTE**

After configuring pool size execute write memory command and restart the router, else it could cause instability on fail over.

**Examples**

The following example shows how to configure a pool size of 200 for transparent VLAN flooding LAG load balancing:

```
device(config)# system-max tvf-lag-lb-fid-pool 200
```

The following example shows how to configure a max pool size of 4096 for transparent VLAN flooding LAG load balancing:

```
device(config)# system-max tvf-lag-lb-fid-pool 4096
```

Reload required. Please write memory and then reload or power cycle the system. Failure to reload could cause system instability on failover. Newly configured `system-max` will not take effect during hitless-reload.

To disable the max pool size configuration use the following command:

```
device(config)# no system-max tvf-lag-lb-fid-pool
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.9.00</td>
<td>This command was modified to add a new FID pool value of 4096.</td>
</tr>
</tbody>
</table>
te-metric

Configures the TE-metric value for an MPLS interface.

Syntax

te-metric value
no te-metric value

Command Default

No TE-metric value is configured.

Parameters

value

Specifies a number for the value of the TE-metric. The value ranges between 1 and 65535.

Modes

MPLS interface configuration mode

Usage Guidelines

no

Examples

The following example sets the TE-metric configured for an MPLS interface to 5.

device# configure terminal
device (config)# router-mpls
device(config-mpls)# mpls-interface ethernet 1/1
device(config-mpls-if-e1000-1/1)# te-metric 5

The following example tries to remove the TE-metric but gives an incorrect value. An error message is displayed that specifies the currently configured value. This correct value is then entered in the no form to remove the TE-metric value for Ethernet interface 1/1.

device# configure terminal
device (config)# router-mpls
device(config-mpls-if-e1000-1/1)#no te-metric 3
Error:TE-metric is configured to a value of 5
device(config-mpls-if-e1000-1/1)#no te-metric 5

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
terminal enable timestamp

Enables and disables the timestamp recording for all show commands for the terminal session of the executed command.

Syntax

```
terminal enable timestamp [ iso8601-format ]
no terminal enable timestamp [ iso8601-format ]
```

Parameters

```
iso8601-format
   Displays the timestamp in ISO 8601 format: YYYY-MM-DDThh:mm:ssTZD (for example, 1997-07-16T19:20:30+01:00). The format uses the following conventions:
   YYYY = Year, four digits
   MM = for example, 01 = January
   DD = Day of the month, two digits (01 through 31)
   hh = Hour, two digits (00 through 23) (am/pm is not allowed)
   mm = Minutes, two digits (00 through 59)
   ss = Seconds, two digits (00 through 59)
   TZD = Time zone designator (Z or +hh:mm or -hh:mm)
```

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to enable the timestamp recording in the default mode to be displayed at the beginning of each show command output. By default, the timestamp is not displayed in the show command outputs. The timestamp recording is applicable only to the current terminal session, and not saved to the startup configuration. The use of this command can assist with troubleshooting or debugging issues.

The default mode is displayed in the system clock format as HH:MM:SS.MSC TZ Wk Mon Day Year (for example 11:41:45.565 GMT+00 Sat Feb 24 2014). The format uses the following conventions:

```
HH = Hour, two digits (00 through 23) (in 24- hour format)
MM = Minutes, two digits (00 through 59)
SS = Seconds, two digits (00 through 59)
MSC = Milliseconds, three digits (000 through 999)
TZ = Time zone
Wk = Weekday, three characters (Sat, Sun, Mon, and so on)
Mon = Month, three characters
Day = Day, two digits (01 through 31)
```
Prior to NetIron OS 5.9.00, some existing show commands (for example, `show tasks` and `show cpu utilization`) displayed the timestamp as part of the show command output. When the `terminal enable timestamp` command is enabled, an additional timestamp recording will now appear at the beginning of the show command outputs on the session where the `terminal enable timestamp` command is issued.

The `no` form of the command disables the timestamp recording at the beginning of each show command output.

### Examples

The following example enables the timestamp recording in default mode. The recording is displayed in the `show ip interface` command output:

```
device# terminal enable timestamp
device# show ip interface
11:41:45.565 GMT+00 Sat Feb 24 2014
Interface         IP-Address      OK?  Method Status     Protocol
VRF
eth 1/2         100.1.1.1       YES  NVRAM  up         up       default-vrf
eth 2/8         216.1.1.1       YES  NVRAM  admin/down down     default-vrf
eth 4/2         42.1.1.1        YES  NVRAM  admin/down down     default-vrf
mgmt 1          10.25.113.41    YES  NVRAM  up         up       default-vrf
ve 10           110.1.1.1       YES  NVRAM  up         up       default-vrf
ve 20           120.1.1.1       YES  NVRAM  up         up       default-vrf
ve 36           36.1.1.1        YES  NVRAM  down       down     default-vrf
ve 44           44.1.1.1        YES  NVRAM  down       down     default-vrf
ve 45           45.1.1.1        YES  NVRAM  down       down     default-vrf
ve 48           48.1.1.1        YES  NVRAM  down       down     default-vrf
```
The following example enables the timestamp recording in the iso8601 format. The recording is displayed in the `show ip interface` command output.

```
device# terminal enable timestamp iso8601-format
device# show ip interface
2014-01-13T19:20:30+01:00

+----------------------------------+-----------------+----------+-------------+-----------------+-----------------+-----------------+
| Secondary | Interface       | IP-Address | OK?  | Method      | Status          | Protocol        |
+----------------------------------+-----------------+----------+----------+-----------------+-----------------+-----------------+
| VRF                                 | eth 2/1         | 21.1.1.5 | YES     | NVRAM         | up              | up              |
| vrf                                 | eth 4/1         | 10.1.1.1 | YES     | manual        | admin/down      | down            |
| vrf1                                | mgmt 1          | 10.37.73.171 | YES | NVRAM | up | up | default- |
| vrf                                 | ve 101          | 11.1.1.1 | YES     | NVRAM         | up              | up              |
| vrf                                 | ve 101          | 11.1.2.1 | YES     | NVRAM         | up              | up              |
| vrf                                 | ve 102          | 12.1.1.1 | YES     | NVRAM         | up              | up              |
| vrf                                 | ve 103          | 13.1.1.1 | YES     | NVRAM         | up              | up              |
| vrf                                 | ve 106          | 16.1.1.1 | YES     | manual        | up              | up              |
+----------------------------------+-----------------+----------+----------+-----------------+-----------------+-----------------+
```

The `show terminal` command is modified to include the terminal timestamp status when the iso8601 format is enabled.

```
device# show terminal
2015-08-03T21:10:59+00:00
Length: 24 lines
Page display mode (session): disabled
Page display mode (global): enabled
Timestamp: enabled (iso8601 format)
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
timers (OSPFv3)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) timers.

Syntax

timers { lsa-group-pacing interval | spf start hold }

Command Default

Enabled.

Parameters

lsa-group-pacing interval

Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check-summed, or aged by the OSPFv3 process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

spf

Specifies start and hold intervals for SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 65535 seconds. The default is 5 seconds.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 65535 seconds. The default is 10 milliseconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

The no timers lsa-group-pacing command restores the pacing interval to its default value.

The no timers spf command sets the SPF timers back to their defaults.
Examples

The following example sets the LSA group pacing interval to 30 seconds.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# timers lsa-group-pacing 30

The following example sets the SPF delay time to 10 and the hold time to 20.

device# configure terminal
device(config)# ipv6 router ospf
device(config-ospf6-router)# timers spf 10 20
traceroute
Traces the network path of packets as they are forwarded to an IPv4 or IPv6 destination address.

Syntax
```
traceroute { ipv4-address | hostname | ipv6 { ipv6-address | ipv6-hostname } } [ maxttl value ] [ minttl value ] [ numeric ] [ source-ip address ] [ timeout seconds ] [ vrf vrf-name ]
```

Parameters
- **ipv4-address**: Specifies the IPv4 address of the destination device.
- **hostname**: Specifies the name of the destination (host) device.
- **ipv6 ipv6-address**: Specifies the IPv6 address of the destination device.
- **ipv6-hostname**: Specifies the name of the destination (host) device.
- **maxttl value**: Maximum TTL value in number of hops.
- **minttl value**: Minimum TTL value in number of hops.
- **numeric**: Displays the IP address in numeric format.
- **source-ip address**: Specifies the IPv4 or IPv6 address of the source device.
- **timeout seconds**: The traceroute timeout value.
- **vrf vrf-name**: Name of the VRF.

Modes
User EXEC mode

Usage Guidelines
Use the `traceroute` command to help troubleshoot networking issues with packets. If no VRF is specified, the default-vrf is used.

If the source address is an IPv6 link-local address, the destination address must be no more than one hop away in the network. An IPv6 link-local address cannot be routed.
Examples

The following example performs an IPv4 traceroute.

device# traceroute 172.16.4.80

traceroute to 172.16.4.80 (172.16.4.80), 64 hops max
1  10.24.80.1 (10.24.80.1) 0.588ms 0.139ms 0.527ms
2  10.31.20.61 (10.31.20.61) 0.550ms 0.254ms 0.234ms
3  10.16.200.113 (10.16.200.113) 0.408ms 0.285ms 0.282ms
4  10.110.111.202 (10.110.111.202) 5.649ms 0.283ms 0.288ms
5  10.150.111.38 (10.150.111.38) 1.108ms 0.712ms 0.704ms
6  10.192.0.42 (10.192.0.42) 37.053ms 32.985ms 41.744ms
7  172.16.56.10 (172.16.56.10) 33.110ms 33.349ms 33.114ms
8  172.16.4.9 (172.16.4.9) 34.096ms 33.023ms 33.122ms
9  172.16.4.80 (172.16.4.80) 76.702ms 83.293ms 79.570ms

The following example performs an IPv6 traceroute, with configured minimum and maximum TTL values and a source IP device address.


History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to add the source-ip option for IPv6.</td>
</tr>
</tbody>
</table>
traceroute mpls ldp

Sends an MPLS echo request from the ingress to the egress Label Switching Router (LSR).

Syntax

```
traceroute mpls ldp { ip_addr/mask_length } [ destination ip_addr ] | [ dsmap ] | [ min-ttl min_num ] | [ max-ttl max_num ] | [ reply-mode router-alert ] | [ reply-tos num ] | [ size bytes ] | [ source ip_addr ] | [ timeout msec ] | [ nexthop ipv4_addr ]
```

Parameters

- **ip_addr mask_length**
  Specifies the LDP IPv4 destination prefix and mask length. If the mask-length is not specified, the default value is 32.

- **destination ip_addr**
  Sets the destination IP address within the 127/8 subset. The default address is 127.0.0.1.

- **dsmap**
  Enables the Downstream (DS) mapping TLV in the echo request for traceroute operation.

- **min-ttl min_num**
  Specifies a minimum value in the min-num variable for the outermost label in the traceroute operation. The default minimum TTL value is one. Acceptable configuration values are 1 - 255.

- **max-ttl max_num**
  Specifies a maximum value in the max-num variable for the outermost label in traceroute operation. The default maximum TTL value is 30. Acceptable configuration values are 1 - 255.

- **reply-mode**
  Used when the normal IP return path is unreliable.

  - **router-alert**
    This option indicates that the reply must be sent as an IPv4 UDP packet with the Router Alert option. This option requires extra overhead processing at each LSR along the return path.

- **reply-tos num**
  Specifies to include a TOS value between 0 and 254 in the Reply-TOS-byte TLV. This value copies to the IP header TOS byte of the echo reply. By default, the reply-tos TLV is not included in the Echo Request.

  **NOTE**
  The last bit of the TOS byte is always zero.

- **size bytes**
  Specifies that the size of the echo request, including the label stack to be sent, and will be the value of the variable bytes. The pad TLV is used to fill the echo request message to the specified size. The minimum size is 92 bytes for an MPLS Echo Request. The maximum size is the size of the LSP MTU.

- **source ip_addr**
  Specifies the IP address of any interface. This address is used as the destination address for the echo reply address. The default address is the LSR ID.

- **timeout msec**
Specifies an interval in milliseconds for the echo request message. The default timeout is five seconds. The maximum timeout value is five minutes.

```
nexthop ipv4_addr
```

Specifies the nexthop IPv4 address that will be used to send the traceroute request. If there is no matching interface for the specified IPv4 address, the traceroute request fails.

**Modes**

Privileged EXEC mode

**Usage Guidelines**

You can specify the nexthop IPv4 address used to send the traceroute request. If there is no matching interface for the specified IPv4 address, the traceroute request fails. When an address that does not match the outgoing path for the tunnel is given, the following error message appears as a response: Traceroute fails: LDP next-hop does not exist.

**Examples**

The following example displays the output returned when using the `traceroute mpls ldp` command.

```
device# traceroute mpls ldp 10.22.22.22
Trace LDP LSP to 10.22.22.22/32, timeout 5000 msec, TTL 1 to 30
Type Control-c to abort
1 10ms 10.22.22.22 return code 3(Egress)
```

**History**

<table>
<thead>
<tr>
<th>Release Version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to include the <code>nexthop</code> keyword.</td>
</tr>
</tbody>
</table>
track-port

Configure network reachability tracking for a specific Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) port.

Syntax

```
track-port { ethernet slot/port | tunnel tunnel-id | ve num } [ priority num ]
```

Command Default

The network reachability of VRRP and VRRP-E ports or IPsec tunnels is not tracked.

Parameters

**ethernet slot/port**

Configure network reachability tracking for a specific Ethernet interface. A forward slash “/” must be entered between the slot and port numbers.

**tunnel tunnel-id**

Configure network reachability tracking for an IPsec tunnel. Valid values range from 1 through 254.

**ve number**

Configure network reachability tracking for a virtual Ethernet interface. Valid values range from 1 through 255.

**priority num**

Sets the track priority. Valid numbers are from 1 through 254. The tracking priority number is used when a tracked interface up or down event is detected. For VRRP, if the tracked interface becomes disabled, the current router priority is reduced to the track-port priority. (For VRRP only, interface tracking does not have any effect on an owner router; the owner priority can not be changed under configuration from 255.) For VRRP-E, if the tracked interface becomes disabled, the current router priority is reduced by the track-port priority. For VRRP, the default is 2, and for VRRP-E, the default is 5.

Modes

```
VRID interface configuration mode
```

Usage Guidelines

This command can be used to track interfaces or IPsec tunnels for VRRP or VRRP-E. IPsec tunnel tracking is supported for IPv4 VRRP and IPv6 VRRP, or IPv4 or IPv6 VRRP-E. IPv6 VRRP does not support IPsec tunnels.

For VRRP, the tracked interface can be any valid Ethernet, or virtual Ethernet interface other than the one on which this command is issued. The maximum number of interfaces you can track per virtual router is 8.

Enter the **no track-port** command with the specified options to remove the tracked port configuration.
Examples

The following example configures network reachability tracking on interface 2/4 and sets the track priority to 60.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# 10.53.5.3/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# track-port ethernet 2/4 priority 60
```

The following example configures network reachability tracking on IPsec tunnels 1 and 2 and sets the track priority to 40 and 20 respectively.

```
device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# 10.53.5.3/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# track-port tunnel 1 priority 40
device(config-if-e1000-1/6-vrid-1)# track-port tunnel 2 priority 20
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>This command was modified to add an option to track IPsec tunnels.</td>
</tr>
</tbody>
</table>
transparent-hw-flooding lag-load-balancing

Configures transparent VLAN flooding LAG load balancing on a specific VLAN when there is PBR to TVF VLAN flooding.

Syntax

transparent-hw-flooding lag-load-balancing

Command Default

By default, transparent VLAN flooding LAG load balancing is not configured on a specific VLAN with flooding.

Modes

VLAN configuration mode

Usage Guidelines

The transparent-hw-flooding lag-load-balancing command configures transparent VLAN flooding LAG load balancing on a specific VLAN when there is PBR to TVF VLAN flooding. The command supports 480 TVF LAG instances.

Use the no form of the command to disable the transparent VLAN flooding LAG load balancing on a specific VLAN.

Examples

The following example enables transparent VLAN flooding LAG load balancing on VLAN 100:

```
device(config)# vlan 100
device(config-vlan-100)# transparent-hw-flooding lag-load-balancing
```

To disable transparent VLAN flooding LAG load balancing on VLAN 100, use the following command:

```
device(config)# vlan 100
device(config-vlan-100)# no transparent-hw-flooding lag-load-balancing
```

History

<table>
<thead>
<tr>
<th>Release Version</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
tunnel destination

Configures the tunnel destination of the tunnel to the specified IPv6 address. IPv6 packets transmitted across the tunnel are received by this address.

Syntax

```plaintext
tunnel destination ipv6-address
no tunnel destination ipv6-address
```

Command Default

This command is not configured.

Parameters

`ipv6-address`
Specifies the IPv6 address to be the destination of the IPsec IPv6 tunnel.

Modes

Tunnel interface configuration mode

Usage Guidelines

The no form of this command removes the specified IPv6 address as the tunnel destination.

Link-local address cannot be used as the destination of the tunnel.

Examples

This example shows configuring the tunnel destination for tunnel number 1 (one) to the IPv6 address of 10:1:1::2/64.

```plaintext
device(config) interface tunnel 1
device(config-tnif-1)# tunnel destination 10:1:1::2/64
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**tunnel mode ipsec ipv4**

Configures the tunnel mode for the specified tunnel to be IPsec IPv4. This enables support for IPSec on the IPv4 packets transmitted across the tunnel.

**Syntax**

```
tunnel mode ipsec ipv4
no tunnel mode ipsec ipv4
```

**Command Default**

IPSec is not supported on IPv4 packets transmitted across a tunnel.

**Modes**

Tunnel interface configuration mode

**Usage Guidelines**

While this command sets IPSec support for IPv4 packets across a tunnel, use the related `tunnel mode ipsec ipv6` command to set IPSec support for IPv6 packets across a tunnel.

The `no` form of this command disables the IPSec IPv4 support on the specified tunnel.

**Examples**

The following example configures the tunnel mode for tunnel number 1 (one) to IPSec IPv4.

```
device# configure terminal
device(config) interface tunnel 1
device(config-tunif-1)# tunnel mode ipsec ipv4
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
tunnel mode ipsec ipv6

Configures the tunnel mode for the specified tunnel to be IPsec IPv6. This enables support for IPSec on the IPv6 packets transmitted across the tunnel.

Syntax

tunnel mode ipsec ipv6

[no] tunnel mode ipsec ipv6

Command Default

This command is not configured.

Modes

Tunnel interface configuration mode

Usage Guidelines

The no form of this command disables the IPSec IPv6 support on the specified tunnel.

Use the tunnel mode ipsec ipv4 command to set the tunnel mode to IPsec IPv4.

Examples

The following example configures the tunnel mode for tunnel number 1 (one) to IPsec IPv6.

device(config) interface tunnel 1
device(config-tun-1)# tunnel mode ipsec ipv6

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
tunnel override-pkt-tos-ttl

Configures the IPsec tunnel to copy the configured TOS and TTL values to the outer IP header.

Syntax

    tunnel override-pkt-tos-ttl
    no tunnel override-pkt-tos-ttl

Command Default

By default, when a packet goes out on an IPsec tunnel, the TOS and TTL values are copied from the inner IP header to the outer IP header.

Modes

Tunnel interface configuration mode

Usage Guidelines

The no form of the command disables the IPsec tunnel from copying the TOS and TTL values.

Examples

The following example configures the IPSec tunnel interface to copy the TOS and TTL values.

device(config)# interface ethernet 3/1
device(config-int-e10000-3/1)# ip address 36.0.8.108/32
device(config-int-e10000-3/1)# interface tunnel 1
device(config-tnif-1)# tunnel override-pkt-tos-ttl

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
tunnel protection ipsec profile

Configures an IPsec profile for an IPsec virtual tunnel interface (VTI).

Syntax

```
tunnel protection ipsec profile ipsec-profile-name
no tunnel protection ipsec profile ipsec-profile-name
```

Command Default

An IPsec profile is not configured for the VTI.

Parameters

`ipsec-profile-name`

Specifies the name of the IPsec profile to secure packets that go out on this interface.

Modes

Interface configuration mode

Usage Guidelines

This command can be used for both IPsec IPv4 and IPsec IPv6 tunnels.

The `no` form of the command removes the IPsec profile configuration.

Examples

The following example shows how to configure an IPsec profile named `ipsec1` on interface 3/1 (the tunnel identifier is 1). This example is for an IPsec IPv4 tunnel.

```
device# configure terminal
device(config)# interface ethernet 3/1
device(config-int-e10000-3/1)# ip address 36.0.8.108/32
device(config-int-e10000-3/1)# interface tunnel 1
device(config-tnif-1)# tunnel protection ipsec profile ipsec1
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.8.00</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>05.9.00</td>
<td>This command was modified to support IPsec IPv6 tunnels.</td>
</tr>
</tbody>
</table>
**tunnel source**

Configures the tunnel source of the tunnel to the specified IPv6 address. IPv6 packets are forwarded from this address across the tunnel.

**Syntax**

```plaintext
tunnel source ipv6-address  
no tunnel source ipv6-address
```

**Command Default**

This command is not configured.

**Parameters**

- **ipv6-address**
  
  Specifies the IPv6 address to be the source of the IPsec IPv6 tunnel.

**Modes**

Tunnel interface configuration mode

**Usage Guidelines**

The `no` form of this command removes the specified IPv6 address as the tunnel source.

Link-local address cannot be used as the source of the tunnel.

**Examples**

This example shows configuring the tunnel source for tunnel number 1 (one) to the IPv6 address of 10:1:1::1/64.

```
device(config) interface tunnel 1  
device(config-tnif-1)# tunnel source 10:1:1::1/64
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
tunnel-interface

Configures the LSP tunnel’s interface index.

Syntax

```
tunnel-interface { index }
no tunnel-interface { index }
```

Command Default

There is no specific default for this command. If not configured, an unused value is chosen.

Parameters

`index`

Decimal value. The range is system dependent. For XMR/MLXe-MR2 systems, the range is 1 - 16384. For CES/CER systems, the range is 1 - 1024.

Modes

MPLS LSP and MPLS bypass LSP modes (config-mpls-lsp).

Usage Guidelines

The `no` option frees the tunnel-interface configured for this node and has a new value dynamically allocated. If the next available index value is the same as that just removed by the user, the same value is still allocated. This is not an error condition. The main purpose of this command is for scenarios where the user wants to allocate any value to the LSP and not something chosen by the user.

The picking algorithm uses the least index that is unused. If none are available (in cases where the number of LSPs supported has been exceeded), the LSP is not allowed to be created. If the user configures a value, there is a check to see if the value is unused or is in use by this tunnel already. If it is in use by another LSP, an error displays and the user will have to configure another value. If it is free, the current value is freed up to be used by any other LSP and the configured value is taken up by this LSP.

This command can be executed irrespective of the state of the LSP - enabled or disabled. It does not depend on adaptive and does not need a commit. The interface index value is for the tunnel and is shared by all the paths - secondary or primary.

Special case handling:

Error handling in the special cases that the user loads a startup-configuration that have the following errors:

1. Multiple LSPs configured with the same tunnel-interface index.
2. In this scenario, the LSPs that comes up later will come up as before.
3. These LSPs do not have a valid tunnel-interface value and cannot be queried using SNMP.
4. In the `show mpls lsp` detail view, the tunnel-interface index is shown as “Invalid”. LSP c2, to 3.3.3.3, tunnel-interface index: Invalid.
4. Only the first LSP to get the value has the valid tunnel-interface index.
5. The configuration continues to show the configured incorrect value, and the user can change it to a valid unused value.
6. The user can list all LSPs that have an invalid tunnel-interface index using the command `show mpls lsp invalid-tunnel-interface`.

2. Multiple LSPs without a tunnel-interface configured.
   a. LSPs that do not have a value configured in the Configuration are allocated to a tunnel-interface index.
   b. It is possible that a later LSP might have configured on it the same value allocated to an LSP as in step 2a.
   c. In such a scenario, de-allocate the index of the first LSP and allocate that value to the later LSP. The former is then allocated a new value from the free indexes.

   NOTE
   The above cases apply *only* to errors in the startup-configuration, not in the case of execution of the CLI during normal running.

Examples

The following example shows how to configure the LSP tunnel interface index:

```plaintext
device#configure terminal
device(config)#router mpls
device(config-mpls)#lsp lsp1
device(config-mpls-lsp1)#tunnel-interface 100
device(config-mpls-lsp1)#to 3.3.3.3
device(config-mpls-lsp1)#enable

device#configure terminal
device(config)#router mpls
device(config-mpls)#bypass-lsp byp1
device(config-mpls-bypasslsp-byp1)#tunnel-interface 102
device(config-mpls-bypasslsp-byp1)#to 3.3.3.3
device(config-mpls-bypasslsp-byp1)#exclude-interface eth 2/1
device(config-mpls-bypasslsp-byp1)#enable
```

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>
**tvf-domain**

Creates a transparent VLAN flooding (TVF) domain that provides an infrastructure to support up to 2016 TVF instances with LAG load balancing.

**Syntax**

```
tvf-domain tvf-domain-ID [ name tvf-domain-name ]
no tvf-domain tvf-domain-ID [ name tvf-domain-name ]
```

**Parameters**

- `tvf-domain-ID` Specifies the ID of the TVF domain. Valid values are from 1 through 2016.
- `name tvf-domain-name` Specifies the name of the TVF domain. The name can be up to 64 characters in length.

**Modes**

Global configuration mode

**Usage Guidelines**

The TVF domain supports only TVF with LAG load balancing.

The no form of the `tvf-domain tvf-domain-ID [ name tvf-domain-name ]` command removes only the name and the TVF domain ID remains the same without a name.

The no form of the `tvf-domain` command removes the TVF domain.

**Examples**

The following example configures a named TVF domain.

```
device# configure terminal
device(config)# tvf-domain 1 name domainuser
```

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**uda access-group**

Binds the user defined ACL table to any physical port.

**Syntax**

```
uda access-group { [ access-list_name | uda-acl num ] [ in ] | enable-deny-logging [ hw-drop ] }
no uda access-group { [ access-list_name | uda-acl num ] [ in ] | enable-deny-logging [ hw-drop ] }
```

**Parameters**

- `access-list_name`
  Specifies the selected access list by name.

- `uda-acl num`
  Specifies the selected UDA access list by the UDA ACL number. The number must be between 2000 - 2999.

- `in`
  Specifies inbound packets.

- `enable-deny-logging`
  Enables UDA ACL logging on the port.

- `hw-drop`
  Drops the ACL deny log packet in the hardware.

**Modes**

User sub-configuration mode (configuration-interface-ethernet).

**Usage Guidelines**

The user defined ACL created must be passed to this CLI command.

Only the user defined ACLs are supported in the ingress side. The UDA offsets must be defined for the access list before binding the ACL to any physical port. If not, the error message "**UDA offsets are not defined for this port**" displays and binding fails.

All the UDA ACL clauses defined in the UDA ACL table are programmed into the hardware. The UDA offsets configured as "ignore" are masked in the ACL rule while programming in the hardware.

If the empty UDA ACL is bound to a physical port, the UDA ACL lookup will not happen until additional rules are added.

The no form of the command removes the binding of the user defined ACL table to any physical port.
Examples

The following example displays the output by number.

device (config)# show access-list uda
UDA Access List 2000:
10: access-list 2000 permit 100 any any 00001122 0000ffff 00003344 0000ffff
20: access-list 2000 permit any any any any any
!
UDA Access List 2001:
10: access-list 2001 permit 200 any any 00001122 0000ffff 00003344 0000ffff
20: access-list 2001 permit any any any any any
!

The following example displays the output by name.

device(config)# show access-list uda TestUdaAcl
UDA Access List TestUdaAcl:
access-list 2000 uda-offsets 12     20     36       72
10: access-list 2000 permit 100 any any 00001122 0000ffff 00003344 0000ffff
20: access-list 2000 permit any any any any any
!

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
uda-offsets

Defines the User Defined fields offset values. This is configured in the physical interface.

Syntax

uda-offsets [ offset0 | ignore ] [ offset1 ignore ] [ offset2 ignore ] [ offset3 ignore ]

no uda-offsets [ offset0 | ignore ] [ offset1 ignore ] [ offset2 ignore ] [ offset3 ignore ]

Command Default

Parameters

offset1
The offset specified is the offset from the beginning of the normalized packet. The maximum value of the offset is 116.

ignore
Ignore offset1.

Modes

User configuration mode (interface-ethernet).

Usage Guidelines

If the offsets are not in the 4 byte boundary or greater than 116, an error message “UDA Offset0 ‘value’ is invalid. The Specify Value is in 32-bit boundary and < 116” displays.

The UDA offsets can be modified when the UDA ACL is bound to the physical port. The UDA ACL rules dynamically update to mask the “ignored” UDA fields.

Deleting uda-offsets when some UDA ACL bound to the physical port is not allowed and an error is displayed (UDA ACL <id> is bound to this port <slot/port>. Unbind UDA ACL before modifying uda-offsets).

The no form of the command removes the uda-offset configuration on the specified UDA Table.

Examples

The following example displays how to define up to four offsets.

device configure terminal
device(config)# interface ethernet 1/1
device(config-intf-e1000-1/1)# uda-offsets 0 4 8 12

The following example displays how to define two offsets.

device configure terminal
device(config)# interface ethernet 1/1
device(config-intf-e1000-1/1)# uda-offsets 0 4 ignore ignore
The following example displays how to remove the uda-offset configuration on the specified UDA table.

device configure terminal
device(config)# interface ethernet 1/1
device(config-intf-e1000-1/1)# no uda-offsets

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was modified to define a User Defined fields offset values.</td>
</tr>
</tbody>
</table>
underflow-limit

Sets the number of consecutive samples which have to be below the threshold value to trigger a premature adjustment to the reserved bandwidth of the label-switched path (LSP).

Syntax

```
underflow-limit value
no underflow-limit value
```

Command Default

The default is that there is no premature adjustment because of underflow.

Parameters

```
value
```

Defines the number of consecutive samples. Default is 0.

Modes

MPLS autobw-template config mode

MPLS LSP mode

Usage Guidelines

In the auto-bandwidth feature, the traffic rate through an LSP is sampled and the reserved bandwidth of the LSP is automatically changed through a make-before-break mechanism. This is done in order to keep the reserved bandwidth close to the actual traffic rate. It is beneficial to have an optimum bandwidth reservation for an LSP. Auto-bandwidth allows for a very efficient use of network-bandwidth. Use the underflow-limit command to reduce the reserved bandwidth prematurely, when the actual traffic rate is consistently much lower than the current reserved bandwidth.

This command can be entered in several modes, under MPLS auto-bandwidth template configuration mode or in MPLS LSP mode as shown in the examples section.

The no function of the command sets the underflow-limit back to the default value.

Examples

The following example sets the underflow-limit in an auto-bandwidth template.

```
device(config)# router mpls
device(config-mpls)# autobw-template template1
device(config-mpls-autobw-template-template1)# underflow-limit 10
```

The following example sets the underflow-limit for an individual LSP.

```
device(config)# router mpls
device(config-mpls)# lsp lsp1
device(config-mpls-lsp-lsp1)# autobw-threshold-table
device(config-mpls-lsp-lsp1-autobw)# underflow-limit 10
```
The following example clears the underflow-limit configuration. The user issues the same command with the `no` option. The underflow-limit configuration is set back to the default value of zero (0).

```
device(config-mpls-autobw-template-template1)# no underflow-limit 10
device(config-mpls-lsp-lsp1-autobw)# no underflow-limit 10
```

**History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6.00</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>
**update-lag-name**

Modifies an existing Link Aggregation Group (LAG) name without deleting and recreating the configured LAG.

**Syntax**

```
update-lag-name new-name
```

**Parameters**

`new-name`

Specifies the new LAG name for an existing LAG name. The LAG name can contain up to 64 characters.

**Modes**

LAG configuration mode

**Usage Guidelines**

The modified LAG name should be unique across all the LAG names that are available. This command works for all LAG types, such as static, dynamic, and keepalive LAGs.

**Examples**

The following example changes the existing LAG name from "blue" to "brocade."

```
device# configure terminal
device(config)# show run
device(config)# lag blue
device(config-lag-blue)# update-lag-name brocade
```

The following partial output verifies the update of the existing LAG name from "blue" to "brocade."

```
device(config)# show run
!Current configuration:
module 3 br-mlx-24-port-1gc-x
!
lag "blue" static id 2
  ports ethernet 3/1
  primary-port 3/1
  deploy
!
! device(config)# lag blue
device(config-lag-blue)# update-lag-name brocade
device(config-lag-brocade)# show run
!Current configuration:
!
module 3 br-mlx-24-port-1gc-x
!
!
lag "brocade" static id 2
  ports ethernet 3/1
  primary-port 3/1
  deploy
```
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.9.00</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
use-v2-checksum

Enables the v2 checksum computation method for an IPv4 Virtual Router Redundancy Protocol version 3 (VRRPv3) session.

Syntax

use-v2-checksum

no use-v2-checksum

Command Default

VRRPv3 uses the v3 checksum computation method.

Modes

VRRP configuration mode

Usage Guidelines

The no form of this command enables the default v3 checksum computation method in VRRPv3 sessions.

Some non-Brocade devices only use the v2 checksum computation method in VRRPv3. This command enables the v2 checksum computation method in VRRPv3 and provides interoperability with these non-Brocade devices.

Examples

The following example shows the v2 checksum computation method enabled for an VRRPv3 IPv4 session on a Brocade device.

device# config
device(config)# router vrrp
device(config)# ethernet 2/4
device(config-if-e1000-2/4)# ip vrrp vrid 14
device(config-if-e1000-2/4-vrid-14)# version v3
device(config-if-e1000-2/4-vrid-14)# use-v2-checksum
device(config-if-e1000-2/4-vrid-14)# activate

History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.00</td>
<td>This command was introduced for IPv6 VRRPv3 sessions running on NetIron device images.</td>
</tr>
<tr>
<td>5.8.00</td>
<td>This command was modified to support IPv4 and IPv6 VRRPv3 sessions running on NetIron device images.</td>
</tr>
</tbody>
</table>
use-vrrp-path

Suppresses RIP advertisements for interfaces on which Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) backup routers are configured.

Syntax

use-vrrp-path

no use-vrrp-path

Command Default

RIP advertisements are sent from the backup router interface.

Modes

RIP router configuration mode

Usage Guidelines

A VRRP backup router includes route information for the interface that is backing up in RIP advertisements. As a result, other routers receive multiple paths for the interface and might unsuccessfully use the path to the backup router rather than the path to the master router. If the VRRP backup routers are suppressed from advertising the backed-up interface in RIP, other routers learn only the path to the master router for the backed-up interface.

The no form of this command resets the default behavior and RIP advertisements are sent from the backup router interface.

Examples

The following example enables RIP advertisement suppression for information about interfaces on VRRP or VRRP-E backup routers.

device# configure terminal
device(config)# router rip
device(config-rip-router)# use-vrrp-path

device(config-rip-router)#

The following example disables RIP advertisement suppression.

device# configure terminal
device(config)# router rip
device(config-rip-router)# no use-vrrp-path

device(config-rip-router)#
version

Sets the version number for a Virtual Router Redundancy Protocol (VRRP) session.

Syntax

version { v2 | v3 }

no version { v2 | v3 }

Command Default

VRRP version 2 is the default.

Parameters

v2

Configures VRRP version 2 for this session.

v3

Configures VRRP version 3 for this session.

Modes

Virtual routing ID interface configuration mode

Usage Guidelines

The no form of this command resets the VRRP session to the default of version 2.

VRRP version 2 supports IPv4 addresses, and VRRP version 3 supports both IPv4 and IPv6 addresses.

NOTE

Mixed mode (VRRPv2 and VRRPv3) is not supported in the same VRRP virtual routing ID (VRID) session.

Examples

The following example sets VRRP routing instance VRID 1 to version 3.

device# configure terminal
device(config)# router vrrp
device(config)# interface ethernet 1/6
device(config-if-e1000-1/6)# ip address 10.53.5.1/24
device(config-if-e1000-1/6)# ip vrrp vrid 1
device(config-if-e1000-1/6-vrid-1)# version v3
virtual-mac

Enables the manual generation of a virtual MAC address for a Virtual Router Redundancy Protocol (VRRP) or VRRP Extended (VRRP-E) instance.

Syntax

```
virtual-mac { mac-address | ipv6-mac-address }
no virtual-mac { mac-address | ipv6-mac-address }
```

Command Default

If there is no manually configured virtual MAC address for a VRRP or VRRP-E instance, the system automatically assigns a virtual MAC address.

Parameters

- `mac-address`
  
  Configures a unique virtual MAC address for an IPv4 VRRP or VRRP-E instance using hexadecimal.

- `ipv6-mac-address`
  
  Configures a unique virtual MAC address for an IPv6 VRRP or VRRP-E instance using hexadecimal.

Modes

VRRP-Extended group configuration mode

Usage Guidelines

By default, the VRRP or VRRP-E virtual MAC is derived as `02:e0:52:<2-byte-ip-hash>:<1-byte-vrid>`.

**NOTE**

System-assigned virtual MAC addresses and manually configured virtual MAC addresses can exist at the same time on the device under the same VRID, but the configured value takes precedence. When the configured value is deleted, the assigned value again applies.

Examples

The following example enables the generation of a virtual MAC with 0 IP hash:

```
device# configure terminal
device(config)# interface ve 10
device(config-ve-10)# vrrp-extended-group 100
device(config-vrrp-extended-group-100)# virtual-mac aaa.bbbb.cccc
```
vll
Defines virtual leased line service and supports inter-operation between vendors.

Syntax
vll name vll_id [ cos num | raw-mode [ cos num ] | raw-pass-through-mode [ cos num ] ]
no vll name vll_id [ cos num | raw-mode [ cos num ] | raw-pass-through-mode [ cos num ] ]

Command Default
A virtual leased line service is not configured.

Parameters
name
The name of the VLL. The name may be up to 64 characters.

vll_id
The VLL identifier. The range is from 1 - 4294967294.

cos num
Optional COS selection.

raw-mode
Raw-mode Ethernet type (VC type 5) (Default is the Tagged mode with VC type 4).

raw-pass-through-mode
Raw-pass-through-mode Ethernet type (VC type 5 if untagged endpoint and VC type 4 if tagged endpoint).

Modes
MPLS configuration mode

Usage Guidelines
The raw-mode and tagged-mode supports are for both CES and XMR platforms. In the raw-pass-through mode, VLL instance behaves similarly to either tagged-mode or raw-mode based on the VLL endpoint configuration and similar to tagged-mode for a tagged endpoint and raw-mode for an untagged endpoint.

Examples
The following example configures the raw-pass-through-mode option.

device(config)#
device(config)# router mpls
device(config-mpls)# soft-preemption cleanup-timer
device(config-mpls)# vll test 1
device(config-mpls)# vll test 1 raw-pass-through-mode
device(config-mpls-vll-test)# vll-peer 10.0.0.1
device(config-mpls-vll-test)# vlan 100
device(config-mpls-vll-test-vlan-100)# tagged ethernet 1/12
device(config-mpls-vll-test-vlan-100)#
## History

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.00</td>
<td>This command was modified to include the <code>raw-pass-through-mode</code> keyword.</td>
</tr>
</tbody>
</table>
vll-peer

Defines the far-end router IP address of the virtual leased line (VLL).

Syntax

vll-peer ip_address [ ip_address | ldp ip_address | lsp lsp_name... ]
no vll-peer ip_address [ ip_address | ldp ip_address | lsp lsp_name... ]

Parameters

ip_address
  Specifies the IP address of the VLL peer.

ldp ip-address
  The destination IP address of an LDP tunnel for the VLL peer.

lsp lsp_name...
  Specifies LSP assignment for the VLL peer.

Modes

MPLS VLL configuration mode

Usage Guidelines

NOTE
  The ldp and lsp options are mutually exclusive; you can configure either the ldp option or the lsp option for a VLL peer.

Use the ldp option to assign a specific LDP tunnel to a VLL.

Use the lsp option to provide a similar user experience as compared to VPLS LSP mapping while at the same time preserving the constructs of VLL peer configurations corresponding to Pseudowire Emulation (PWE) redundancy and MCT-VLL. This approach is backwards compatible. Incremental additions and deletions are allowed.

Up to eight LSP names to a peer can be configured using this command. All eight LSPs are optional. When a VLL peer is not assigned to any LSPs, the default mechanisms for selecting an LSP for the VLL peer are used.

To verify the configuration of this command, use the show mpls config vll command with the name of the VLL for which you want to display the configuration.

The no form of the command removes the far-end router IP address configuration for a virtual leased line (VLL).
Examples

The following example shows how to assign a specific LDP tunnel to a VLL.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 10.1.1.1 ldp 10.5.5.5
device# show mpls config vll test
vll test 1000
  vll-peer 10.1.1.1 ldp 10.5.5.5
  vlan 1000
tagged e 4/5
```

The following example configures a single VLL peer with a set of LSPs.

```
NOTE
Configuring the VLL peer and assigning LSPs can be done in the same line.
```

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
device# show mpls config vll test
vll test 1000
  vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
  vlan 1000
tagged e 4/5
```

The following example appends an LSP to an existing list of LSPs mapped to a VLL peer.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp5
```

The following example removes an LSP from an existing list of LSPs for a VLL peer.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3 lsp4
device(config-mpls-vll-test)# no vll-peer 1.1.1.1 lsp lsp4
device(config-mpls-vll-test)# end
device# show mpls config vll test
vll test 45000
  vll-peer 1.1.1.1 lsp lsp1 lsp2 lsp3
  vlan 1000
tagged e 4/5
```

The following example configures primary and standby VLL peers with a set of LSPs.

```
NOTE
When configuring LSPs for primary or standby peers, it is mandatory to configure the peers in advance and then proceed to configure the respective LSPs.
```

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 2.2.2.2
device(config-mpls-vll-test)# vll-peer 1.1.1.1 lsp lspa1 lspa2 lspa3 lspa4
device(config-mpls-vll-test)# vll-peer 2.2.2.2 lsp lspa1 lspa2 lspa3 lspa4
```
The following example removes an LSP from the list of LSPs mapped to a standby VLL peer.

device# configure terminal
device(config)# router mpls
device(config-mpls)# vll test 1000
device(config-mpls-vll-test)# vll-peer 1.1.1.1 2.2.2.2
device(config-mpls-vll-test)# vll-peer 2.2.2.2 lsp lspa1 lspa2 lspa3 lspa4
device(config-mpls-vll-test)# no vll-peer 2.2.2.2 lsp lspa4

---

**History**

<table>
<thead>
<tr>
<th>Release version</th>
<th>Command history</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7.0</td>
<td>This command was modified to add the <code>lsp</code> keyword to assign mapped LSPs to the VLL. Up to eight LSPs are now available.</td>
</tr>
<tr>
<td>6.0.0</td>
<td>This command was modified to add the <code>ldp</code> keyword. The <code>ldp</code> keyword assigns a specific LDP tunnel to a VLL.</td>
</tr>
</tbody>
</table>

---

**Object Missing**

This object is not available in the repository.
write memory

Saves the current running configuration information to the startup configuration file.

Syntax

```
write memory
```

Command Default

Configuration information is not saved to the startup-config file until a `write memory` is performed.

Modes

- Privileged EXEC mode

Usage Guidelines

This command saves a configuration change permanently so that the change remains in effect following a system reset or software reload. This command can be entered in any configuration mode, as well as in Privileged EXEC mode.

Some configuration changes like memory allocation changes, require you to reload the software after you save the changes to the startup configuration file.

You should always execute the `write memory` command after making extensive configuration changes. For example, on devices that support stacking any stacking-related configuration changes such as changing priority or stacking ports should be saved to the startup-config file.

**NOTE**

Keep a backup copy of the startup configuration file in the event of system reset.

Examples

The following example configures a new priority of 255 for stack unit 1, enables the priority, and saves the configuration change to the startup configuration file.

```
device# config terminal
device(config)# stack unit 1
device(config-unit-1)# priority 255
device(config-unit-1)# stack enable
Enable stacking. This unit actively participates in stacking
device(config-unit-1)# write memory
Write startup-config done.
Flash Memory Write (8192 bytes per dot) .Flash to Flash Done.
device(config-unit-1)# end
```