

# Extreme SLX-OS Command Reference, 16r.1.01

Supporting the ExtremeRouting SLX 9850 Router

© 2018, Extreme Networks, Inc. All Rights Reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks). Specifications and product availability are subject to change without notice.

© 2017, Brocade Communications Systems, Inc. All Rights Reserved.

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

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

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

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

# Contents

---

<b>Preface</b> .....	<b>23</b>
Document conventions.....	23
Notes, cautions, and warnings.....	23
Text formatting conventions.....	23
Command syntax conventions.....	24
Extreme resources.....	24
Document feedback.....	24
Contacting Extreme Technical Support.....	25
<b>About This Document</b> .....	<b>27</b>
What's new in this document.....	27
New commands.....	27
Modified commands.....	27
Supported hardware and software.....	28
<b>Commands A - B</b> .....	<b>29</b>
aaa accounting.....	29
aaa authentication .....	31
acl-mirror.....	33
acl-policy.....	35
action python-script.....	36
adaptive.....	38
address-family l2vpn evpn (BGP).....	39
address-family unicast (BGP).....	40
address-family unicast (IS-IS).....	42
adjustment-interval.....	43
adjustment-threshold.....	44
admin-group.....	45
advertise dot1-tlv .....	47
advertise dot3-tlv .....	48
advertise-backup .....	49
advertise optional-tlv .....	50
advertisement-interval (VRRP).....	52
advertisement-interval-scale .....	54
aggregate-address (BGP).....	55
alias .....	57
alias-config .....	59
allow-conflicting-rules.....	60
allow-duplicate-rules.....	62
always-compare-med .....	64
always-propagate .....	65
anycast-rp.....	67
area authentication (OSPFv3).....	69
area nssa (OSPFv2).....	71
area nssa (OSPFv3).....	73
area prefix-list (OSPFv2).....	75
area range (OSPFv2).....	77

area range (OSPFv3).....	79
area stub (OSPFv2).....	81
area stub (OSPFv3).....	83
area virtual-link authentication (OSPFv3).....	85
area virtual-link (OSPFv2).....	87
area virtual-link (OSPFv3).....	89
arp .....	91
as-path-ignore .....	93
auth-check.....	94
auth-key.....	96
auth-mode.....	98
auto-cost reference-bandwidth (OSPFv2).....	100
auto-cost reference-bandwidth (OSPFv3).....	102
auto-shutdown-new-neighbors.....	104
backup-advertisement-interval .....	105
bandwidth-ceiling.....	106
banner.....	108
bgp-redistribute-internal .....	109
bpdu-drop-enable.....	110
breakout mode 4x10g.....	111
bridge-domain.....	112
bridge-priority .....	114
bsr-candidate.....	116
<b>Commands C - D.....</b>	<b>119</b>
capability as4-enable .....	119
certutil import sshkey .....	120
chassis .....	122
cisco-interoperability .....	124
class .....	125
class-map .....	127
clear arp .....	128
clear counters .....	129
clear counters access-list .....	130
clear counters access-list overlay type vxlan .....	132
clear counters storm-control .....	133
clear dot1x statistics .....	135
clear ip bgp dampening .....	136
clear ip bgp flap-statistics .....	137
clear ip bgp local routes .....	138
clear ip bgp neighbor .....	139
clear ip bgp routes .....	141
clear ip bgp traffic .....	142
clear ip dhcp relay statistics .....	143
clear ip ospf .....	144
clear ip route .....	146
clear ipv6 bgp dampening .....	147
clear ipv6 bgp flap-statistics .....	148
clear ipv6 bgp local routes .....	149
clear ipv6 bgp neighbor.....	150
clear ipv6 bgp routes.....	152

clear ipv6 bgp traffic.....	153
clear ipv6 counters .....	154
clear ipv6 dhcp relay statistics .....	155
clear ipv6 neighbor.....	156
clear ipv6 ospf .....	157
clear ipv6 route.....	159
clear ipv6 vrrp statistics .....	160
clear isis all .....	162
clear isis counts .....	163
clear isis database .....	164
clear isis force-spf .....	165
clear isis force-v6spf .....	166
clear isis ipv6 spf-log .....	167
clear isis neighbor .....	168
clear isis route .....	169
clear isis spf-log .....	170
clear isis traffic .....	171
clear lldp neighbors.....	172
clear lldp statistics.....	174
clear mac-address-table.....	176
clear mpls auto-bandwidth-samples.....	178
clear mpls lsp.....	179
clear mpls statistics.....	180
clear openflow .....	182
clear policy-map-counters .....	183
clear statistics bridge-domain.....	184
clear statistics openflow .....	185
clear statistics vlan.....	186
clear tm voq-stat ingress-device.....	187
clear tm voq-stat slot .....	188
clear tunnel statistics.....	189
clear vrrp statistics.....	190
CLI.....	192
client.....	195
client-interface.....	196
client-interfaces-shutdown.....	197
client-isolation-strict.....	198
client-to-client-reflection .....	199
cluster.....	200
cluster-id .....	201
compare-med-empty-aspath .....	202
compare-routerid .....	203
confederation identifier.....	204
confederation peers.....	205
configure terminal .....	206
conform-set-dscp .....	207
conform-set-prec .....	208
conform-set-tc .....	209
connector.....	210
copy .....	211

cos.....	213
crypto ca authenticate.....	214
crypto ca enroll.....	216
crypto ca import.....	218
crypto ca trustpoint.....	220
crypto key .....	221
csnp-interval.....	223
cspf-computation-mode.....	224
cspf-interface-constraint.....	226
cspf-group.....	227
cspf-group-computation.....	228
dampening .....	229
database-overflow-interval (OSPFv2).....	231
database-overflow-interval (OSPFv3).....	233
debug access-list-log buffer .....	235
debug dhcp packet buffer .....	236
debug ip bgp .....	238
debug ip bgp neighbor .....	240
debug ip igmp .....	242
debug ip pim .....	244
debug ipv6 bgp.....	246
debug ipv6 bgp neighbor.....	248
debug udld packet .....	250
default-information-originate (BGP).....	252
default-information-originate (IS-IS).....	253
default-information-originate (OSPFv2).....	254
default-information-originate (OSPFv3).....	256
default-link-metric.....	258
default-local-preference .....	260
default-metric (BGP).....	261
default-metric (IS-IS).....	262
default-metric (OSPF).....	263
default-passive-interface .....	264
delay.....	265
delay-link-event.....	266
delete .....	268
deploy.....	269
designated-forwarder-hold-time.....	270
description.....	271
description (LLDP).....	272
description (STP).....	273
description (VRRP).....	274
destination .....	275
dir .....	276
disable-adjacency-check.....	277
disable-incremental-spf-opt.....	278
disable-inc-stct-spf-opt.....	279
disable-partial-spf-opt.....	280
distance (BGP).....	281
distance (IS-IS).....	282

distance (OSPF).....	283
distribute-list prefix-list (OSPFv3).....	285
distribute-list route-map .....	286
dot1x authentication .....	287
dot1x enable.....	288
dot1x filter-strict-security.....	289
dot1x max-req .....	291
dot1x port-control.....	292
dot1x reauthenticate .....	294
dot1x reauthentication .....	295
dot1x reauthMax .....	296
dot1x quiet-period .....	297
dot1x test eapol-capable .....	298
dot1x test timeout .....	299
dot1x timeout .....	300
dscp.....	302
dscp-ttl-mode.....	303
<b>Commands E - F.....</b>	<b>305</b>
ebs .....	305
eir .....	306
enforce-first-as .....	307
eol.....	308
error-disable-timeout enable .....	309
error-disable-timeout interval .....	310
esi.....	312
event-handler.....	313
clear event-handler action.....	315
event-handler activate.....	316
exceed-set-dscp .....	319
exceed-set-prec .....	320
exceed-set-tc .....	321
external-lsdb-limit (OSPFv2).....	322
external-lsdb-limit (OSPFv3).....	323
exclude-any.....	324
fast-external-fallover .....	325
fast-flood.....	326
fastboot.....	327
filter-fec-in.....	328
filter-fec-out.....	330
forward-delay .....	331
from.....	333
<b>Commands G - J.....</b>	<b>335</b>
graceful-restart (BGP).....	335
graceful-restart (LDP).....	338
graceful-restart (OSPFv2).....	339
graceful-restart helper (OSPFv3).....	341
graceful-restart helper-disable (IS-IS).....	342
handle-isis-neighbor-down.....	343
ha chassisreboot .....	345

ha disable .....	346
ha enable .....	347
ha failover .....	348
ha sync start .....	349
ha sync stop .....	350
hardware.....	351
hello (LLDP).....	352
hello (MPLS RSVP).....	354
hello (UDLD).....	356
hello-acknowledgements.....	357
hello-interval (LDP) .....	358
hello-interval (PIM).....	359
hello-interval-link .....	360
hello-interval-target .....	361
hello-time .....	362
hello-timeout (LDP) .....	364
hello-timeout-link .....	365
hello-timeout-target .....	366
hello padding.....	367
helper-only.....	369
hold-time .....	370
hop-limit.....	371
hostname disable.....	372
implicit-commit.....	373
inactivity-timer.....	374
include-all.....	375
include-any.....	376
ingress-tunnel-accounting.....	377
install-igp-cost .....	378
instance .....	379
interface management.....	381
interval.....	382
ip access-group .....	383
ip access-list .....	385
ip address .....	387
ip arp-aging-timeout .....	389
ip dhcp relay address .....	391
ip dhcp relay gateway address.....	392
ip dns .....	393
ip icmp rate-limiting .....	394
ip icmp redirect.....	395
ip igmp immediate-leave .....	396
ip igmp last-member-query-interval .....	397
ip igmp query-interval .....	398
ip igmp query-max-response-time .....	399
ip igmp router-alert-check-disable.....	400
ip igmp snooping enable .....	401
ip igmp snooping fast-leave .....	402
ip igmp snooping last-member-query-interval.....	403
ip igmp snooping mrouter interface .....	404



ip igmp snooping querier enable .....	405
ip igmp snooping query-interval.....	406
ip igmp snooping query-max-response-time.....	407
ip igmp snooping static-group.....	408
ip igmp ssm-map.....	409
ip igmp static-group .....	411
ip igmp version.....	412
ip mtu .....	413
ip ospf active .....	414
ip ospf area .....	415
ip ospf auth-change-wait-time .....	416
ip ospf authentication-key .....	418
ip ospf cost .....	419
ip ospf database-filter .....	420
ip ospf dead-interval .....	422
ip ospf hello-interval .....	424
ip ospf ldp-sync .....	426
ip ospf md5-authentication .....	427
ip ospf mtu-ignore .....	429
ip ospf network .....	430
ip ospf passive .....	432
ip ospf priority .....	433
ip ospf retransmit-interval .....	434
ip ospf transmit-delay .....	435
ip pim dr-priority.....	436
ip pim-sparse .....	438
ip pim ttl-threshold.....	439
ip policy route-map.....	440
ip proxy-arp .....	441
ip receive access-group.....	442
ip route.....	444
ip router-id .....	446
ip router isis .....	447
ip vrrp-extended auth-type .....	448
ipv6 access-group .....	450
ipv6 access-list .....	452
ipv6 address.....	454
ipv6 dhcp relay address .....	456
ipv6 dns .....	458
ipv6 icmpv6 rate-limiting .....	459
ipv6 mtu .....	460
ipv6 ospf active .....	461
ipv6 ospf area .....	462
ipv6 ospf authentication ipsec .....	463
ipv6 ospf authentication ipsec disable .....	464
ipv6 ospf authentication spi.....	465
ipv6 ospf cost .....	467
ipv6 ospf dead-interval .....	468
ipv6 ospf hello-interval .....	469
ipv6 ospf hello-jitter .....	471

ipv6 ospf instance .....	472
ipv6 ospf mtu-ignore .....	473
ipv6 ospf network .....	474
ipv6 ospf passive .....	476
ipv6 ospf priority .....	477
ipv6 ospf retransmit-interval .....	478
ipv6 ospf suppress-linklsa .....	479
ipv6 ospf transmit-delay .....	480
ipv6 policy route-map.....	481
ipv6 prefix-list.....	482
ipv6 protocol vrrp .....	484
ipv6 protocol vrrp-extended .....	485
ipv6 receive access-group.....	486
ipv6 route.....	488
ipv6 route next-hop-vrf.....	490
ipv6 route null.....	492
ipv6 router isis .....	494
ipv6 router ospf .....	495
ipv6 vrrp-extended auth-type .....	496
ipv6 vrrp-extended-group .....	497
ipv6 vrrp-group .....	498
ipv6 vrrp-suppress-interface-ra .....	499
isis auth-check.....	500
isis auth-key.....	502
isis auth-mode.....	503
isis circuit-type.....	504
isis hello-interval.....	505
isis hello-multiplier.....	507
isis hello padding.....	509
isis ipv6 metric.....	510
isis ldp-sync.....	512
isis metric.....	513
isis passive.....	515
isis point-to-point.....	516
isis priority.....	517
isis reverse-metric.....	519
is-type.....	521
iterations.....	523
<b>Commands K - M.....</b>	<b>525</b>
ka-int-count.....	525
ka-interval.....	526
ka-timeout.....	528
key-add-remove-interval.....	530
key-rollover-interval.....	531
keypair.....	533
label-withdrawal-delay .....	534
ldp.....	535
ldp-enable.....	536
ldp-params.....	537
ldp-sync.....	538

link-error-disable.....	540
link-fault-signal.....	542
load-sharing.....	544
local-as .....	545
local-switching.....	546
log (OSPFv2).....	547
log (OSPFv3).....	549
log adjacency.....	551
log-dampening-debug .....	552
log invalid-lsp-packets.....	553
log-shell.....	554
logical-interface (bridge domain).....	555
lsp.....	557
lsp-gen-interval.....	558
lsp-interval.....	559
lsp-refresh-interval.....	560
lsp-id .....	561
mac access-group .....	562
mac access-list extended .....	564
mac access-list standard .....	566
master-vlan (STP).....	567
match (route map).....	568
match access-group .....	572
maxas-limit .....	573
maximum-paths (BGP).....	574
maximum-paths (IS-IS).....	576
maximum-paths (OSPF).....	577
maximum-paths ebgp ibgp .....	578
max-age .....	580
max-lsp-lifetime.....	582
max-mcache .....	583
max-metric router-lsa .....	584
max-metric router-lsa (OSPFv3).....	586
max-neighbor-reconnect-time.....	588
max-neighbor-recovery-time.....	589
med-missing-as-worst .....	590
member-bridge-domain.....	591
member vlan.....	592
member-vlan (STP).....	594
message-interval .....	595
metric.....	596
metric-style wide.....	597
metric-type .....	598
mode gre ip .....	599
mode (LLDP) .....	600
mode (port-group).....	601
mpls-interface.....	602
mpls reoptimize.....	603
mtu.....	604
mtu-enforce.....	605

multipath .....	606
multiplier (LLDP).....	608
multiplier (UDLD).....	609
multi-topology.....	610
<b>Commands N - Q.....</b>	<b>613</b>
nbr-timeout .....	613
neighbor activate.....	614
neighbor advertisement-interval .....	616
neighbor allowas-in .....	618
neighbor as-override .....	620
neighbor capability as4 .....	622
neighbor capability orf prefixlist.....	624
neighbor default-originate .....	626
neighbor description .....	628
neighbor ebgp-btsh .....	630
neighbor ebgp-multihop .....	632
neighbor enforce-first-as .....	634
neighbor filter-list .....	636
neighbor local-as .....	638
neighbor maxas-limit in .....	640
neighbor maximum-prefix .....	642
neighbor next-hop-self .....	644
neighbor password .....	646
neighbor peer-group .....	648
neighbor prefix-list .....	650
neighbor remote-as .....	652
neighbor remove-private-as.....	654
neighbor route-map .....	656
neighbor route-reflector-client .....	658
neighbor send-community .....	660
neighbor shutdown .....	662
neighbor soft-reconfiguration inbound .....	664
neighbor static-network-edge.....	666
neighbor timers .....	668
neighbor unsuppress-map .....	670
neighbor update-source .....	672
neighbor weight .....	674
net.....	676
network .....	677
next-hop-enable-default .....	679
next-hop-mpls.....	680
next-hop-recursion .....	682
node.....	683
nonstop-routing (IS-IS).....	684
nonstop-routing (OSPF).....	685
notification-timer.....	686
openflow default-behavior send-to-controller .....	687
openflow enable .....	688
openflow-controller.....	690
openflow protected-vlans.....	692

oscmd.....	694
overlay access-group.....	696
overlay access-list type vxlan extended.....	697
overlay access-list type vxlan standard .....	698
overlay-transit.....	699
partial-spf-interval.....	700
password-attributes .....	702
path.....	705
peer.....	707
peer (MCT).....	709
peer-interface.....	710
penalty.....	711
police cir.....	712
policy-map .....	714
port-channel path-cost .....	716
port-group.....	718
power-off.....	719
power-on.....	720
preempt-mode .....	721
priority .....	722
process-restart.....	724
profile .....	725
protocol.....	727
protocol lldp .....	728
protocol spanning-tree .....	729
protocol udd .....	731
protocol vrrp .....	732
protocol vrrp-extended .....	733
prune-wait.....	734
pw-profile.....	735
pw-profile (bridge domain).....	737
python.....	738
qos cos .....	742
qos cos-mutation .....	743
qos cos-traffic-class.....	744
qos cpu slot .....	745
qos dscp-cos .....	747
qos dscp-mutation .....	748
qos dscp-traffic-class .....	749
qos map cos-mutation .....	750
qos map cos-traffic-class.....	752
qos map dscp-cos .....	754
qos map dscp-mutation .....	756
qos map dscp-traffic-class .....	758
qos map traffic-class-cos .....	760
qos-mpls map dscp-exp.....	762
qos-mpls map exp-dscp .....	764
qos-mpls map exp-traffic-class .....	766
qos-mpls map traffic-class-exp.....	768
qos-mpls map-apply dscp-exp.....	770

qos-mpls map-apply exp-dscp.....	771
qos-mpls map-apply exp-traffic-class.....	772
qos-mpls map-apply traffic-class-exp.....	773
qos rx-queue cos-threshold .....	774
qos rx-queue multicast best-effort-rate.....	775
qos rx-queue multicast guarantee-rate.....	776
qos rx-queue multicast traffic-class .....	777
qos rx-queue unicast traffic-class.....	778
qos service-policy.....	779
qos traffic-class .....	780
qos traffic-class-cos.....	781
qos tx-queue scheduler strict-priority .....	782
<b>Commands R - Sh.....</b>	<b>785</b>
radius-server .....	785
reconnect-time.....	787
recovery-time.....	788
redistribute .....	789
refresh-reduction.....	793
region .....	795
reliable-messaging.....	796
reload.....	798
rename .....	799
reoptimize-timer.....	800
resequence access-list .....	801
reservable-bandwidth.....	803
retransmit-interval.....	805
retry-limit.....	806
retry-time.....	807
reverse-metric.....	808
revert-timer.....	810
revertive global.....	812
revertive hold-time.....	814
revision .....	815
rfc1583-compatibility (OSPF).....	816
rib-route-limit .....	817
rmon alarm .....	819
rmon collection history .....	821
rmon collection stats .....	823
rmon event .....	824
role name .....	826
router bgp .....	828
router isis .....	829
router mpls.....	830
router ospf .....	831
router pim.....	832
route-precedence.....	833
rp-address.....	834
rp-candidate.....	836
rpf ecmp rebalance.....	838
rsvp.....	839

rsvp-flooding-threshold.....	840
rsvp-periodic-flooding-time.....	842
rule .....	843
rx-label-silence-time.....	845
sample-recording.....	846
seq (rules in IPv4 extended ACLs).....	847
seq (rules in IPv4 standard ACLs).....	852
seq (rules in IPv6 extended ACLs).....	854
seq (rules in IPv6 standard ACLs).....	859
seq (rules in MAC extended ACLs).....	862
seq (rules in MAC standard ACLs).....	866
service password-encryption .....	868
service-policy .....	869
session.....	871
set-debug.....	873
set extcommunity.....	874
set ip interface null0 .....	876
set ip next-hop .....	877
set ipv6 interface null0 .....	878
set ipv6 next-hop .....	879
set-overload-bit.....	880
sflow enable (global version).....	882
sflow polling-interval (global version).....	883
sflow sample-rate (global version).....	884
shutdown (STP).....	885
<b>Show A through Show I.....</b>	<b>887</b>
show access-list.....	887
show access-list-log buffer .....	890
show access-list-log buffer config.....	892
show access-list overlay transit.....	893
show access-list overlay type vxlan acl-name .....	894
show arp .....	895
show bridge-domain.....	897
show cluster.....	902
show crypto ca .....	904
show crypto key.....	906
show default threshold .....	907
show dot1x .....	909
show event-handler activations.....	912
show file .....	914
show ha.....	916
show hardware port-group.....	917
show interface stats brief.....	918
show interface stats detail.....	920
show access-list overlay transit.....	922
show ip bgp.....	923
show ip bgp attribute-entries .....	924
show ip bgp dampened-paths .....	925
show ip bgp filtered-routes .....	926
show ip bgp flap-statistics .....	927

show ip bgp neighbors .....	929
show ip bgp neighbors advertised-routes .....	931
show ip bgp neighbors flap-statistics .....	932
show ip bgp neighbors last-packet-with-error.....	933
show ip bgp neighbors received .....	935
show ip bgp neighbors received-routes .....	936
show ip bgp neighbors rib-out-routes.....	937
show ip bgp neighbors routes .....	938
show ip bgp neighbors routes-summary .....	939
show ip bgp peer-group .....	940
show ip bgp routes .....	941
show ip bgp routes community .....	944
show ip bgp summary .....	945
show ip dhcp relay address interface .....	946
show ip dhcp relay gateway.....	947
show ip dhcp relay statistics .....	948
show ip igmp groups .....	949
show ip igmp interface .....	950
show ip igmp snooping .....	951
show ip igmp ssm-map.....	952
show ip igmp statistics vlan.....	953
show ip igmp statistics interface .....	954
show ip interface .....	955
show ip multicast snooping.....	957
show ip ospf .....	958
show ip ospf area .....	959
show ip ospf border-routers .....	961
show ip ospf config .....	962
show ip ospf database .....	963
show ip ospf filtered-lsa area .....	966
show ip ospf interface .....	967
show ip ospf neighbor .....	969
show ip ospf redistribute route .....	970
show ip ospf routes .....	971
show ip ospf summary .....	973
show ip ospf traffic .....	974
show ip ospf virtual link .....	976
show ip ospf virtual neighbor .....	977
show ip pim bsr.....	978
show ip pim interface.....	981
show ip pim mcache .....	982
show ip pim neighbor.....	983
show ip pim rp-candidate.....	985
show ip pim rp-hash.....	987
show ip pim rp-map.....	988
show ip pim rp-set.....	989
show ip pim rpf.....	991
show ip pim traffic.....	992
show ip route .....	994
show ipv6 bgp.....	998



show ipv6 bgp attribute-entries .....	999
show ipv6 bgp dampened-paths .....	1000
show ipv6 bgp filtered-routes .....	1001
show ipv6 bgp flap-statistics .....	1002
show ipv6 bgp neighbors .....	1004
show ipv6 bgp neighbors advertised-routes .....	1006
show ipv6 bgp neighbors flap-statistics .....	1007
show ipv6 bgp neighbors last-packet-with-error.....	1008
show ipv6 bgp neighbors received .....	1010
show ipv6 bgp neighbors received-routes .....	1011
show ipv6 bgp neighbors rib-out-routes.....	1012
show ipv6 bgp neighbors routes.....	1013
show ipv6 bgp neighbors routes-summary.....	1014
show ipv6 bgp peer-group .....	1017
show ipv6 bgp routes .....	1018
show ipv6 bgp routes community .....	1021
show ipv6 bgp summary .....	1022
show ipv6 counters interface .....	1023
show ipv6 dhcp relay address interface .....	1024
show ipv6 dhcp relay statistics .....	1025
show ipv6 interface .....	1026
show ipv6 nd .....	1028
show ipv6 neighbor.....	1030
show ipv6 ospf .....	1031
show ipv6 ospf area .....	1032
show ipv6 ospf database .....	1033
show ipv6 ospf interface .....	1036
show ipv6 ospf memory .....	1037
show ipv6 ospf neighbor .....	1038
show ipv6 ospf redistribute route .....	1040
show ipv6 ospf routes .....	1041
show ipv6 ospf spf .....	1042
show ipv6 ospf summary .....	1043
show ipv6 ospf virtual-links .....	1044
show ipv6 ospf virtual-neighbor .....	1045
show ipv6 prefix-list.....	1046
show ipv6 route .....	1047
show ipv6 static route .....	1049
show ipv6 vrrp .....	1050
show isis.....	1055
show isis config.....	1059
show isis counts.....	1060
show isis database .....	1063
show isis hostname.....	1066
show isis interface .....	1067
show isis neighbors .....	1073
show isis routes .....	1076
show isis spf-log .....	1078
show isis traffic .....	1081
show port-security .....	1083

<b>Show J through Show Z.....</b>	<b>1085</b>
show lldp interface .....	1085
show lldp neighbors.....	1087
show lldp statistics.....	1089
show mac-address-table.....	1090
show mpls autobw-threshold-table.....	1093
show mpls lsp.....	1094
show mpls policy.....	1098
show mpls rsvp.....	1099
show mpls rsvp interface.....	1101
show mpls statistics.....	1104
show mpls te database.....	1107
show openflow .....	1109
show openflow controller.....	1112
show openflow flow .....	1113
show openflow group .....	1115
show openflow interface .....	1117
show openflow meter .....	1118
show openflow queues .....	1119
show openflow resources .....	1121
show policy-map .....	1123
show port-security .....	1125
show qos cpu cfg.....	1127
show qos cpu info.....	1130
show qos interface all.....	1131
show qos interface ethernet .....	1135
show qos interface port-channel.....	1138
show qos interface ve.....	1145
show qos maps cos-traffic-class .....	1147
show qos maps dscp-cos .....	1148
show qos maps dscp-mutation .....	1149
show qos maps dscp-traffic-class .....	1150
show qos maps traffic-class-cos.....	1151
show qos-mpls maps dscp-exp.....	1152
show qos-mpls maps exp-dscp.....	1153
show qos-mpls maps exp-traffic-class .....	1154
show qos-mpls maps traffic-class-exp.....	1155
show route-map .....	1156
show run router mpls cspf-group.....	1158
show running-config .....	1159
show running-config aaa .....	1160
show running-config aaa accounting .....	1162
show running-config access-list overlay type vxlan.....	1163
show running-config event-handler.....	1164
show running-config ip access-list .....	1166
show running-config ipv6 .....	1167
show running-config ipv6 access-list .....	1169
show running-config mac access-list.....	1170
show running-config password-attributes .....	1171
show running-config radius-server .....	1173

show running-config rmon .....	1174
show running-config role .....	1175
show running-config rule .....	1176
show running-config ssh .....	1178
show running-config ssh server .....	1179
show running-config ssh server key-exchange .....	1180
show running-config username .....	1181
show sflow .....	1183
show slots.....	1184
show spanning-tree .....	1186
show startup-config .....	1188
show statistics access-list .....	1189
<b>show statistics access-list overlay type vxlan .....</b>	<b>1191</b>
show statistics bridge-domain.....	1192
show statistics vlan.....	1194
show storm-control .....	1196
show tm voq-stat ingress-device all discards.....	1198
show tm voq-stat ingress-device ethernet.....	1200
show tm voq-stat slot.....	1202
show topology-group.....	1205
show tunnel.....	1207
show tunnel statistics.....	1208
show udd .....	1209
show udd interface .....	1210
show udd statistics .....	1212
show users .....	1213
show vrrp.....	1214
<b>Commands Si - Z.....</b>	<b>1219</b>
snmp-server community.....	1219
snmp-server contact.....	1220
snmp-server context.....	1222
snmp-server enable trap.....	1224
snmp-server engineid local .....	1225
snmp-server group .....	1226
snmp-server host .....	1228
snmp-server location.....	1230
snmp-server mib community-map.....	1232
snmp-server sys-descr.....	1234
snmp-server user .....	1236
snmp-server v3host .....	1239
snmp-server view .....	1241
soft-preemption.....	1243
soft-preemption cleanup-timer.....	1244
source .....	1245
spanning-tree autoedge .....	1247
spanning-tree bpdu-mac .....	1248
spanning-tree cost .....	1249
spanning-tree edgeport .....	1250
spanning-tree guard root .....	1252
spanning-tree link-type .....	1253

spanning-tree portfast .....	1254
spanning-tree priority .....	1256
spanning-tree restricted-role .....	1257
spanning-tree restricted-tcn .....	1258
spanning-tree shutdown .....	1259
speed (Ethernet).....	1260
spf-interval.....	1262
spt-threshold.....	1264
ssh .....	1265
ssh client cipher.....	1268
ssh client cipher non-cbc.....	1269
ssh client key-exchange .....	1270
ssh client mac.....	1271
ssh server cipher.....	1272
ssh server cipher non-cbc.....	1273
ssh server key.....	1274
ssh server key-exchange .....	1276
ssh server mac.....	1277
ssh server max-sessions.....	1278
ssh server rekey-interval .....	1280
ssh server shutdown .....	1281
ssh server standby enable.....	1282
ssm-enable.....	1283
start-shell.....	1285
static-network .....	1286
statistics .....	1287
statistics (bridge domain).....	1288
statistics (VLAN).....	1289
storm-control ingress .....	1290
subnet.....	1292
summary-address (IS-IS).....	1293
summary-address (OSPFv2).....	1295
summary-address (OSPFv3).....	1297
summary-prefix.....	1299
switch-attributes.....	1301
switchport port-security .....	1303
switchport port-security mac-address .....	1304
switchport port-security max .....	1305
switchport port-security shutdown-time .....	1306
switchport port-security sticky .....	1307
switchport port-security violation .....	1308
system-description .....	1309
system-name .....	1310
table-map .....	1311
tacacs-server .....	1313
telnet.....	1315
telnet server.....	1317
terminal.....	1319
threshold-monitor cpu .....	1321
threshold-monitor memory .....	1323

threshold-monitor sfp .....	1325
tie-breaking.....	1328
timers (BGP).....	1329
timers (OSPFv2).....	1331
timers (OSPFv3).....	1333
topology-group.....	1335
traceroute .....	1336
track (VRRP).....	1338
traffic-engineering.....	1340
traffic-engineering (LSP).....	1342
transit-session-accounting.....	1344
trigger.....	1345
trigger-function.....	1347
trigger-mode.....	1349
ttd.....	1351
tx-label-silence-timer.....	1352
udld enable .....	1353
underflow-limit.....	1354
unlock username .....	1355
update-time .....	1356
use-v2-checksum.....	1358
user (alias configuration).....	1359
username .....	1360
vc-id.....	1362
vc-mode.....	1363
virtual-ip .....	1365
virtual-mac .....	1367
vrrp-extended-group .....	1368
vrrp-group .....	1369



# Preface

---

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

## Document conventions

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

## Notes, cautions, and warnings

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

### NOTE

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

### ATTENTION

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



### CAUTION

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



### DANGER

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

## Text formatting conventions

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

Format	Description
<b>bold text</b>	Identifies command names. Identifies keywords and operands. Identifies the names of GUI elements.
<i>italic text</i>	Identifies text to enter in the GUI. Identifies emphasis. Identifies variables.
Courier font	Identifies document titles. Identifies CLI output.

Format	Description
	Identifies command syntax examples.

## Command syntax conventions

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

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.  Default responses to system prompts are enclosed in square brackets.
{ x   y   z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x   y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	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.

## Extreme resources

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

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at [www.extremenetworks.com](http://www.extremenetworks.com). Product documentation for all supported releases is available to registered users at [www.extremenetworks.com/support/documentation](http://www.extremenetworks.com/support/documentation).

## Document feedback

Quality is our first concern at Extreme, 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:

- Use our short online feedback form at <http://www.extremenetworks.com/documentation-feedback-pdf/>
- Email us at [internalinfodev@extremenetworks.com](mailto:internalinfodev@extremenetworks.com)

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



# Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

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

- [GTAC \(Global Technical Assistance Center\)](#) for immediate support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact).
  - Email: [support@extremenetworks.com](mailto:support@extremenetworks.com). To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) - Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers



# About This Document

---

- [What's new in this document.....](#) 27
- [Supported hardware and software.....](#) 28

## What's new in this document

This document is the *Extreme SLX-OS Command Reference* for the SLX 9850 Router.

### NOTE

On October 30, 2017, Extreme Networks, Inc. acquired the data center networking business from Brocade Communications Systems, Inc. This document has been updated to remove or replace references to Brocade Communications, Inc. with Extreme Networks, Inc., as appropriate.

In the initial release of the command reference, not all commands supported on the device are represented. For new commands introduced since Release 16r.1.01, the history table is shown.

Information has been added or updated to reflect enhancements to existing features for the SLX 9850 Router.

## New commands

The following commands are new in this document:

- `protocol`
- `show ha`

## Modified commands

The following commands have been modified in this document:

- `event handler abort action`
- `ha disable`
- `ha enable`
- `ha chassisreboot`
- `ha failover`
- `ha sync start`
- `ha sync stop`
- `oscmd`
- `show udl interface`

# Supported hardware and software

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

Although many different software and hardware configurations are tested and supported by Extreme Networks, Inc. for SLX-OS Release 16r.1.01, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- ExtremeRouting SLX 9850-4
- ExtremeRouting SLX 9850-8

# Commands A - B

---

## aaa accounting

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

### Syntax

```
aaa accounting {commands defaultstart-stop [none | tacacs+] | execdefaultstart-stop [none | tacacs+]}
```

```
no aaa accounting {commands defaultstart-stop [none | tacacs+] | execdefaultstart-stop [none | tacacs+]}
```

### Parameters

#### commands

Toggles the logging of commands.

#### exec

Toggles the logging of login information.

#### default

Sends the logged information to the default server.

#### start-stop

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

#### tacacs+

Sends the logged information to the TACACS+ server.

#### none

Disables accounting services.

### Modes

Global configuration mode

### Usage Guidelines

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

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

### Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# aaa authentication

Configures the AAA login sequence.

## Syntax

```
aaa authentication login { default | ldap | local }
aaa authentication login { radius | tacacs+ } { local | local-auth-fallback }
no aaa authentication login
```

## Command Default

The default server is Local.

## Parameters

### login

Specifies the type of server that will be used for authentication, authorization, and accounting (AAA) on the device. The local server is the default. Specify one of the following options:

#### default

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

#### ldap

Specifies the Lightweight Directory Access Protocol (LDAP) servers.

#### local

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

#### radius

Specifies the RADIUS servers.

#### tacacs+

Specifies the TACACS+ servers.

#### local

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

#### local-auth-fallback

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

## Modes

Global configuration mode

## Usage Guidelines

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

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

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

## Examples

To change the AAA server to TACACS+ using the local device database as a secondary source of authentication:

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# acl-mirror

Defines a destination port or port-channel for ACL-based mirroring of a physical interface.

## Syntax

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

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

## Command Default

No ACL mirror is defined.

## Parameters

### source

Specifies the interface for which you are defining a mirror.

### ethernet

Specifies a physical Ethernet interface.

#### *slot*

Specifies a valid slot number.

#### *port*

Specifies a valid port number.

### destination

Specifies the physical interface or port-channel mirror.

### ethernet

Specifies a physical Ethernet interface.

#### *slot*

Specifies a valid slot number.

#### *port*

Specifies a valid port number.

### port-channel *index*

Specifies a port-channel interface.

## Modes

Global configuration mode

## Usage Guidelines

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

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

Although in an extended-ACL rule you can specify **mirror**, **log**, and **copy-sflow**, only one of the three is processed, as follows:

- In a permit rule, the order of precedence is **mirror > copy-sflow > log**.
- In a deny or hard-drop rule, the order of precedence is **log > copy-sflow > mirror**.

The destination port must be on the same chip as the source port.

Only one destination port is supported per chip.

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

## Examples

The following example defines a physical port as mirror.

```
device# configure
device(config)# acl-mirror source ethernet 2/1 destination ethernet 3/2
```

The following example defines a port-channel as mirror.

```
device# configure
device(config)# acl-mirror source ethernet 3/1 destination port-channel 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# acl-policy

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

## Syntax

```
acl-policy
```

## Modes

Global configuration mode

## Usage Guidelines

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# action python-script

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

## Syntax

**action python-script** *file-name*

**no action python-script** *file-name*

## Parameters

*file-name*

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

## Modes

Event-handler configuration mode

## Usage Guidelines

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

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

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

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

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

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

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# adaptive

When a parameter is changed on an adaptive LSP, a new instance of the same LSP is signaled using the newly defined parameters. Once the new LSP comes up, traffic is moved to the new LSP instance and the old LSP instance is torn down.

## Syntax

```
adaptive
no adaptive
```

## Command Default

By default, LSPs are not adaptive.

## Modes

MPLS LSP configuration mode (`config-router-mpls-lsp-lsp_name`).

## Usage Guidelines

### NOTE

The new parameters are not changed for the adaptive LSP until the **commit** command is issued for the LSP.

### NOTE

Once the **commit** command has been issued, there may be a 30 ms traffic disruption.

The **no** form of the command removes the adaptive LSP.

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# address-family l2vpn evpn (BGP)

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

## Syntax

`address-family l2vpn evpn`

`no address-family l2vpn evpn`

## Command Default

Disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

This example enables BGP address family L2VPN EVPN configuration mode.

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

## History

Release version	Command history
16r.1.01	This command was introduced.

# address-family unicast (BGP)

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

## Syntax

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

## Command Default

Disabled.

## Parameters

**ipv4**  
Specifies an IPv4 address family.

**ipv6**  
Specifies an IPv6 address family.

**vrf vrf-name**  
Specifies a VRF instance.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

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

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

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

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



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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# address-family unicast (IS-IS)

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

## Syntax

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

## Command Default

Disabled.

## Parameters

**ipv4**  
Specifies the IPv4 address family.

**ipv6**  
Specifies the IPv6 address family.

## Modes

IS-IS router configuration mode

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# adjustment-interval

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

## Syntax

```
adjustment-interval { value }
```

```
no adjustment-interval { value }
```

## Command Default

The adjustment-interval is disabled.

## Parameters

*value*

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

## Modes

MPLS LSP configuration mode.

## Usage Guidelines

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# adjustment-threshold

To specify the sensitivity of the automatic bandwidth adjustment of an LSP to changes in bandwidth utilization, use the **adjustment-threshold** command. This command is used to set the threshold for when to trigger automatic bandwidth adjustments. When automatic bandwidth adjustment is configured, bandwidth demand for the current interval is determined and compared to the LSPs current bandwidth allocation.

## **adjustment-threshold use-threshold-table**

### **no adjustment-threshold**

The adjustment threshold is set to the default value.

### **use-threshold-table**

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

MPLS sub-configuration modes.

config-mpls-template-template1

config-mpls-lsp-lsp1-autobw

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

Release version	Command history
16r.1.00	This command was introduced.

# admin-group

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

## Syntax

```
admin-group { admin_name admin_group_num }
no admin-group { admin_name admin_group_num }
```

## Command Default

The command is disabled, by default.

## Parameters

*admin\_name*

Specifies the selected administrative group name.

*admin\_group\_number*

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

## Modes

MPLS policy mode.

## Usage Guidelines

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

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

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

## Examples

The following example establishes three administrative groups.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# advertise dot1-tlv

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

## Syntax

```
advertise dot1-tlv
```

```
no advertise dot1-tlv
```

## Command Default

Advertisement is disabled.

## Modes

Protocol LLDP and profile configuration modes

## Usage Guidelines

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

## Examples

The following example advertises TLV configuration for IEEE 802.1

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# advertise dot3-tlv

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

## Syntax

```
advertise dot3-tlv
no advertise dot3-tlv
```

## Command Default

Advertisement is disabled.

## Modes

Protocol LLDP and profile configuration modes.

## Usage Guidelines

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

## Examples

The following example advertises TLV configuration for IEEE 802.3.

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# advertise-backup

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

## Syntax

```
advertise-backup
no advertise-backup
```

## Command Default

Advertisement is disabled.

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

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

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

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

## Examples

To enable the backup VRRP routers to send advertisement frames to the master VRRP router:

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# advertise optional-tlv

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

## Syntax

```
advertise optional-tlv { management-address | port-description | system-capabilities | system-description | system-name }  
no advertise optional-tlv
```

## Command Default

Advertisement is disabled.

## Parameters

### management-address

Advertises the management address of the system.

### port-description

Advertises the user-configured port.

### system-capabilities

Advertises the capabilities of the system.

### system-description

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

### system-name

Advertises the name of the system.

## Modes

Protocol LLDP and profile configuration modes

## Usage Guidelines

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# advertisement-interval (VRRP)

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

## Syntax

`advertisement-interval` *range*

## Command Default

1 second for version 2, 1000 milliseconds for version 3.

## Parameters

*range*

Interval at which the master VRRP router advertises its existence to the backup routers. Valid values range from 1 through 255 seconds for VRRPv2 and from 100 through 40900 milliseconds for VRRPv3.

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

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

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# advertisement-interval-scale

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

## Syntax

**advertisement-interval-scale** *scale*

## Command Default

The default advertisement interval scale is 1.

## Parameters

*scale*

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

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

This command scales the advertisement interval of the master VRRP-Ev3 device as configured by the **advertisement-interval** command. A value of 1, 2, 5, or 10 can be set and the existing advertisement interval value is divided by the scaling value, for example, if the advertisement interval is set to 1 second and the scaling value is set to 10, the new advertisement interval is 100 milliseconds. When all the advertisement intervals in a VRRP-Ev3 session are scaled, subsecond VRRP-Ev3 convergence is possible if a master fails. The advertisement notifies the backup devices that the master is still active. If the backup devices do not receive an advertisement from the master in a designated amount of time, the backup device with the highest priority can assume the role of master. Using subsecond advertising intervals, subsecond device redundancy can be achieved.

This command is only supported by VRRP-Ev3.

## Examples

To set the scaling of the advertisement interval to 500 milliseconds for VRRP-Ev3 group 19:

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# aggregate-address (BGP)

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

## Syntax

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

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

## Command Default

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

## Parameters

*ip-addr*

IPv4 address.

*ip-mask*

IPv4 mask.

*ipv6-addr*

IPv6 address.

*ipv6-mask*

IPv6 mask.

### **advertise-map**

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

*map-name*

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

### **as-set**

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

### **attribute-map**

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

*map-name*

Specifies a route map to be consulted.

### **summary-only**

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

### **suppress-map**

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

*map-name*

Specifies a route map to be consulted.

## Modes

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

## Usage Guidelines

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# alias

Configures global or user-level aliases for device commands.

## Syntax

**alias** *alias-name expansion*

**no alias** *alias-name*

## Parameters

*alias-name*

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

*expansion*

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

## Modes

Alias configuration mode

User-alias configuration mode

## Usage Guidelines

Global aliases are available to all users.

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

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

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# alias-config

Launches the alias configuration mode, enabling you to define aliases. The **no** versions of this command enable you to delete all global aliases or all aliases defined for a specified user.

## Syntax

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

## Parameters

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

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

## Modes

Global configuration mode

## Usage Guidelines

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

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

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# allow-conflicting-rules

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

## Syntax

`allow-conflicting-rules`

`no allow-conflicting-rules`

## Command Default

Conflicting rules are not allowed within an ACL.

## Modes

ACL policy mode

## Usage Guidelines

If the only difference between two rules is that one is a **deny** and the other a **hard-drop**, they are not considered conflicting. However, they are considered duplicates; refer to [allow-duplicate-rules](#) on page 62.

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

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

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

## Examples

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

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

```
device# show running-config mac access-list extended macl
mac access-list extended macl
  seq 10 permit host 0001.0001.0001 any
  seq 20 deny host 0001.0001.0002 any count
  seq 30 hard-drop host 0001.0001.0003 any mirror
```

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

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

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# allow-duplicate-rules

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

## Syntax

`allow-duplicate-rules`

`no allow-duplicate-rules`

## Command Default

Duplicate rules are not allowed within an ACL.

## Modes

ACL policy mode

## Usage Guidelines

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

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

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

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

## Examples

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

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

```
device# show running-config mac access-list extended macl
mac access-list extended macl
  seq 10 permit host 0001.0001.0001 any
  seq 20 deny host 0001.0001.0002 any count
  seq 30 hard-drop host 0001.0001.0003 any mirror
```

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

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

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# always-compare-med

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

## Syntax

```
always-compare-med
no always-compare-med
```

## Command Default

This feature is disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

This example configures the device always to compare the MEDs.

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# always-propagate

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

## Syntax

**always-propagate**

**no always-propagate**

## Command Default

This feature is disabled.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

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

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

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# anycast-rp

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

## Syntax

**anycast-rp** *rp-address*

**no anycast-rp** *rp-address*

## Command Default

PIM anycast RPs are not configured.

## Parameters

*rp-address*

Specifies a shared RP address used among multiple PIM routers.

## Modes

PIM router configuration mode

## Usage Guidelines

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

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

When the source is activated in a PIM Anycast RP domain, the PIM First Hop (FH) will register the source to the closet PIM RP. The PIM RP follows the same MSDP Anycast RP operation by decapsulating the packet and creating the (s,g) state. If there are external peers in the Anycast RP set, the router will re-encapsulate the packet with the local peering address as the source address of the encapsulation. The router will unicast the packet to all Anycast RP peers. The re-encapsulation of the data register packet to Anycast RP peers ensures source state distribution to all RPs in a multicast domain.

## Examples

The following example shows how to configure PIM anycast RP.

```
device(config-pim-router)# anycast-rp101.101.101.101 my-anycast-rps
device(config-pim-router)# exit
device(config)# ip prefix-list my-anycast-rpspermit 1.1.1.1/32
device(config)# ip prefix-list my-anycast-rpspermit 2.2.2.2/32
device(config)# interface loopback 1
device(config-Loopback-1)# ip address 1.1.1.1/32
device(config-Loopback-1)# ip pim-sparse
device(config)#interface loopback 2
device(config-Loopback-2)# ip address 2.2.2.2/32
device(config-Loopback-2)# ip pim-sparse
device(config-Loopback-11)# ip address 101.101.101.101/32
device(config-Loopback-11# ip pim-sparse
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# area authentication (OSPFv3)

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

## Syntax

```
area { A.B.C.D | decimal } authentication spi value { ah | esp null } { hmac-md5 | hmac-sha1 } key key
no area { A.B.C.D | decimal } authentication spi value
```

## Command Default

Authentication is not enabled on an area.

## Parameters

*A.B.C.D*

Area address in dotted decimal format.

*decimal*

Area address in decimal format.

**spi**

Specifies the Security Policy Index (SPI).

*value*

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

**ah**

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

**esp**

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

**null**

Specifies that the ESP payload is not encrypted.

**hmac-md5**

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

**hmac-sha1**

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

**key**

Number used in the calculation of the message digest.

*key*

The 40 hexadecimal character key.

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# area nssa (OSPFv2)

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

## Syntax

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

## Command Default

No areas are created.

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

*metric*

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

**no-summary**

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

**Note:** This parameter is disabled by default, which means the default route must use a Type 7 LSA.

**default-information-originate**

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

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

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

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# area nssa (OSPFv3)

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

## Syntax

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

```
no area nssa
```

## Command Default

No areas are created.

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

*metric*

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

### default-information-originate

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

### metric-type

Specifies how the cost of a neighbor metric is determined.

#### type1

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

#### type2

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

### no-redistribution

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

### no-summary

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

**Note:** This parameter is disabled by default, which means the default route must use a Type 7 LSA.

**translator-always**

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

**translator-interval** *interval*

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

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

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

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# area prefix-list (OSPFv2)

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

## Syntax

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

## Command Default

Disabled.

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

**prefix-list** *name*

Specifies a prefix-list.

**in**

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

**out**

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

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# area range (OSPFv2)

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

## Syntax

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

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

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

**no area range**

## Parameters

*A.B.C.D*

Area address in IP address format.

*decimal*

Area address in decimal format.

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

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

**advertise**

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

**cost** *cost\_value*

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

**not-advertise**

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

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

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

An example of when you might want to use this command is if you have many small networks advertised from area 0 to any other area, or from any non-backbone area into the backbone. This command gives you a summary route instead of many

smaller routes. In an area, the OSPF database on each router must be an exact copy of the databases of the other routers. This means that no summarization is allowed within the area.

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# area range (OSPFv3)

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

## Syntax

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

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

*ipv6 address/mask*

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

**advertise**

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

**cost** *cost\_value*

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

**not-advertise**

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

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

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

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# area stub (OSPFv2)

Creates or deletes a stub area or modifies its parameters.

## Syntax

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

## Command Default

No areas are created.

## Parameters

*A.B.C.D*

Area address in IP address format.

*decimal*

Area address in decimal format.

*metric*

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

**no-summary**

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

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# area stub (OSPFv3)

Creates or deletes a stub area or modifies its parameters.

## Syntax

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

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

**no area stub**

## Command Default

No areas are created.

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

*metric*

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

**no-summary**

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

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# area virtual-link authentication (OSPFv3)

Enables authentication for virtual links in an OSPFv3 area.

## Syntax

```
area { ip-addr | decimal } virtual-link E.F.G.H authentication spi spi-value { ah | esp null } { hmac-md5 | hmac-sha1 } key key
no area { A.B.C.D | decimal } virtual-link E.F.G.H authentication spi spi
```

## Command Default

Authentication is not enabled on a virtual-link.

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

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

*E.F.G.H*

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

spi *spi-value*

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

ah

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

esp

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

null

Specifies that the ESP payload is not encrypted.

hmac-md5

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

hmac-sha1

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

key *key*

Number used in the calculation of the message digest.40 hexadecimal character key.

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# area virtual-link (OSPFv2)

Creates or modifies virtual links for an area.

## Syntax

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

```
no area virtual-link
```

## Command Default

No virtual links are created.

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

*E.F.G.H*

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

**authentication-key** *password*

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

**dead-interval** *time*

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

**hello-interval** *time*

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

**md5-authentication**

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

**key-activation-wait-time** *time*

Time before a newly configured MD5 authentication key is valid. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends will use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes (300 seconds) after the new MD5 key is in operation. Valid values range from 0 through 14400 seconds. The default is 300 seconds.

**key-id** *num key*

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

**retransmit-interval** *time*

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

**transmit-delay** *time*

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

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# area virtual-link (OSPFv3)

Creates or modifies virtual links for an area.

## Syntax

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

```
no area virtual-link
```

## Command Default

No virtual links are created.

## Parameters

*ip-addr*

Area address in IP address format.

*decimal*

Area address in decimal format.

*A.B.C.D*

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

**dead-interval** *time*

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

**hello-interval** *time*

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

**hello-jitter** *interval*

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

**retransmit-interval** *time*

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

**transmit-delay** *time*

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

## Modes

- OSPFv3 router configuration mode
- OSPFv3 router VRF configuration mode

## Usage Guidelines

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

## arp

Specifies the IPv4 and MAC address for a static address resolution protocol (ARP) entry.

## Syntax

```
arp A.B.C.D mac_address interface { ethernet slot / port | ve ve_id }
no arp A.B.C.D
```

## Parameters

*A.B.C.D*

A valid IP address.

*mac\_address*

A valid MAC address.

**ethernet**

Specifies a physical Ethernet interface.

*slot*

Specifies a valid slot number.

*port*

Specifies a valid port number.

**ve** *ve\_id*

Specifies a virtual ethernet (VE) interface.

## Modes

Global configuration mode

VRF configuration mode

## Usage Guidelines

To delete a static ARP, use the **no** form of this command.

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# as-path-ignore

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

## Syntax

`as-path-ignore`

`no as-path-ignore`

## Command Default

This feature is disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# auth-check

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

## Syntax

```
auth-check { level-1 | level-2 } disable
no auth-check { level-1 | level-2 }
```

## Command Default

IS-IS authentication checking is enabled by default.

## Parameters

**level-1**  
Specifies Level 1 packets only.

**level-2**  
Specifies Level 2 packets only.

**disable**  
Disables authentication checking.

## Modes

IS-IS router configuration mode

## Usage Guidelines

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

## Examples

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

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

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# auth-key

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

## Syntax

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

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

## Command Default

No authentication key is configured.

## Parameters

### level-1

Specifies Level 1 packets only.

### level-2

Specifies Level 2 packets only.

### string

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

## Modes

IS-IS router configuration mode

## Usage Guidelines

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

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

## Examples

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

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

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

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



# History

Release version	Command history
16r.1.00	This command was introduced.

# auth-mode

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

## Syntax

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

## Command Default

Disabled.

## Parameters

**md5**  
Specifies Message Digest 5 (MD5) authentication.

**level-1**  
Specifies Level 1 packets only.

**level-2**  
Specifies Level 2 packets only.

## Modes

IS-IS router configuration mode

## Usage Guidelines

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# auto-cost reference-bandwidth (OSPFv2)

Configures reference bandwidth.

## Syntax

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

## 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-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500
```

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# auto-cost reference-bandwidth (OSPFv3)

Configures reference bandwidth.

## Syntax

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

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

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

### NOTE

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

The **no** form of the command restores the reference bandwidth to its default value and, thus, restores the default costs of the interfaces to their default values.

## Examples

The following example configures a reference bandwidth of 500.

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# auto-shutdown-new-neighbors

Disables the establishment of BGP connections with a remote peer when the peer is first configured.

## Syntax

```
auto-shutdown-new-neighbors
no auto-shutdown-new-neighbors
```

## Command Default

This feature is disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

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

## Examples

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

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

The following example disables the peer shutdown state and begins the BGP4 session establishment process.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65520
device(config-bgp-router)# no neighbor 10.1.1.1 shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# backup-advertisement-interval

Configures the interval at which backup VRRP routers advertise their existence to the master router.

## Syntax

`backup-advertisement-interval interval`

## Command Default

The default backup advertisement-interval is 60 seconds.

## Parameters

*interval*

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

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

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

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

## Examples

To set the backup advertisement interval to 120 seconds for VRRP-E group 10:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# backup-advertisement-interval 120
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# bandwidth-ceiling

This command adds a new threshold change point to the autobw-threshold table. When the change point is already there, the threshold value updates to the new value.

## Syntax

```
bandwidth-ceiling [ bw in kbps | max ] threshold [ threshold _n_kbps | [ percentage threshold_percentage ] ]
no bandwidth-ceiling
```

## Command Default

There are no bandwidth ceiling entry.

## Parameters

*bw\_in\_kbps*

The bandwidth in kilobytes per second. 0 - 0x7FFFFFFF. Range of bandwidth in kbps.

**max**

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

**threshold** *theshold \_in\_kbps*

The threshold in kilobytes per second. 0 - 0x7FFFFFFF. Range of bandwidth in kbps.

**threshold** *threshold\_percentage*

The threshold percentage per second. 0 - 100%. By default, the last ceiling is used.

### NOTE

The first parameter indicates that any rate above the maximum ceiling configured. The second parameter is the threshold in kbps. for those rates.

## Modes

MPLS global adjustment threshold configuration mode.

## Usage Guidelines

Review the updated global adjustment-threshold table after executing this command.

The **max** keyword sets the threshold for any traffic-rate above the maximum bandwidth-ceiling configured in the table.

The **no** function of the command remove the bandwidth ceiling entry from the table.

## Examples

```
device#
```

Release version	Command history
16r.1.00	This command was introduced.

# banner

Defines an incoming, login, or message of the day banner.

## Syntax

```
banner { incoming | login | motd } string
no banner incoming | login | motd
```

## Parameters

### incoming

Sets the incoming terminal line banner that is displayed on the console when a user establishes a Telnet session.

### login

Sets the login banner that is displayed on the user terminal when the user logs into the device.

### motd

Sets the message of the day (MOTD) that is displayed on the user terminal when a Telnet CLI session is established.

### *string*

Specifies a text string from 1 through 2048 characters in length including spaces.

## Modes

Global configuration mode.

## Usage Guidelines

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

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

## Examples

To create a login banner with a single line:

```
device(config)# banner login "Please do not disturb the setup on this switch"
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# bgp-redistribute-internal

Causes the device to allow the redistribution of IBGP routes from BGP into OSPF for non-default VRF instances.

## Syntax

**bgp-redistribute-internal**

**no bgp-redistribute-internal**

## Command Default

This feature is disabled.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

By default, with default VRF instances, the device does not allow the redistribution of IBGP routes from BGP4 and BGP4+ into OSPF. This helps to eliminate routing loops. In non-default VRF instances, use this command to allow the redistribution of IBGP routes from BGP into OSPF. This command is enabled only if a non-default VRF instance has been specified.

## Examples

This example enables BGP4 route redistribution.

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

This example enables BGP4+ route redistribution for VRF instance "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# bpdu-drop-enable

Enables dropping Layer 2 (L2) bridge protocol data units (BPDUs) on endpoints in a bridge domain.

## Syntax

**bpdu-drop-enable**

**no bpdu-drop-enable**

## Command Default

Dropping of L2 BPDUs is disabled. L2 BPDUs are allowed on endpoints in the bridge domain.

## Modes

Bridge-domain configuration mode.

## Usage Guidelines

The **no** form of the command disables dropping of Layer 2 (L2) bridge protocol data units (BPDUs) in a bridge domain.

## Examples

The following example shows how to enable dropping of L2 BPDUs in bridge domain 3.

```
device# configure terminal
device(config)# bridge-domain 3
device(config-bridge-domain-3)# bpdu-drop-enable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# breakout mode 4x10g

Configures any 40G port on the SLX 9850 36X100G line card (LC) as four 10G ports.

## Syntax

```
breakout mode 4x10g
```

```
no breakout mode 4x10g
```

## Modes

Hardware connector configuration mode

## Usage Guidelines

Use the **no** form of the command to reset the port on the 36X100G LC to a 40G port.

You must power off the line card before using this command.

After using this command, save the running-config file to the startup-config file, and power on the line card or reload the device for the changes to take effect.

When you power on the line card, the SFP interfaces come up under the new mode with default configurations. Unaffected interfaces retain the configurations they had before the line card was powered off.

## Examples

The following example shows the configuration of a 40G port on the 36X100G LC into four 10G ports.

```
device# power-off linecard 4
device# configure terminal
device(config)# hardware
device(config-hardware)# connector 4/2
device(config-connector-4/2)# breakout mode 4x10g
%Warning: Sfp Breakout is a disruptive command.
Please save the running-config to startup-config and use reload command on the device or power-cycle
linecard on Chassis system for the changes to take effect.
device(config-port-group-4/2)# Ctrl-z
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
device# power-on linecard 4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# bridge-domain

Creates a bridge domain. A bridge domain represents a switching or inter-connection domain for a wide range of service end-point types.

## Syntax

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

## Command Default

No bridge domain is configured.

## Parameters

*id*  
Specifies a unique numeric bridge-domain identifier. The range is from 1 through 4096.

**p2mp**  
Specifies a multipoint service type. This is the default service type.

**p2p**  
Specifies a point-to-point cross-connect service type.

## Modes

Global configuration mode.

## Usage Guidelines

VPLS performs any-to-any switching between Ethernet attachment circuits (ACs) and MPLS pseudowires (PWs). VLL performs one-to-one switching between Ethernet AC and MPLS PWs. Use the bridge-domain to specify the related configuration for both VPLS and VLL.

The **no** version of the command removes the bridge-domain configuration.

## Examples

The following example shows how to configure bridge domain 1 and specifies a point-to-point cross-connect service for the domain.

```
device# configure terminal
device(config)# bridge-domain 1 p2p
```

The following example shows the error message that is displayed when the specified bridge-domain ID is out of range.

```
device# configure terminal
device(config)# bridge-domain 10000000
Error: syntax error: "10000000" is out of range.
```



The following example shows the error message that is displayed when the bridge-domain creation is not successful in the back-end.

```
device# configure terminal
device(config)# bridge-domain 110
Error: bridge-domain: connection instance creation failed.
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# bridge-priority

Specifies the bridge priority for the common instance.

## Syntax

**bridge-priority** *priority*

**no bridge-priority**

## Command Default

The default priority is 32768.

## Parameters

*priority*

Specifies the bridge priority. Valid values range from 0 through 61440 in increments of 4096.

## Modes

Protocol Spanning Tree mode

## Usage Guidelines

The priority values can be set only in increments of 4096.

Using a lower priority value indicates that the bridge might become root.

Enter **no bridge-priority** to return to the default priority.

## Examples

To specify the bridge priority:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# bridge-priority 8192
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# bridge-priority 8192
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# bridge-priority 8192
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## bsr-candidate

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

### Syntax

```
bsr-candidate interface [ ethernet | loopback | port-channel | ve ]
no bsr-candidate
```

### Command Default

The PIM router does not participate in BSR election.

### Parameters

**loopback** *num*  
Specifies the loopback interface for the candidate BSR.

**ve** *num*  
Specifies the virtual interface for the candidate BSR.

**port-channel** *num*  
Specifies the port-channel number for the candidate BSR.

### Modes

PIM Router configuration mode

### Usage Guidelines

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

Each PIM Sparse domain has one active BSR. For redundancy, you can configure ports on multiple devices as candidate BSRs. The PIM Sparse protocol uses an election process to select one of the candidate BSRs as the BSR for the domain. The BSR with the highest BSR priority is elected. If the priorities result in a tie, the candidate BSR interface with the highest IP address is elected.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

### Examples

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

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

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# Commands C - D

---

## capability as4-enable

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

### Syntax

`capability as4-enable`

`no capability`

### Command Default

This feature is disabled.

### Modes

BGP configuration mode

### Usage Guidelines

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

### Examples

The following example enables 4-byte ASN capability.

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

### History

Release version	Command history
16r.1.00	This command was introduced.

# certutil import sshkey

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

## Syntax

```
certutil import sshkey host remote_ip_address directory ssh_public_key_path user user_acct password password login
login_id
```

```
no certutil sshkey
```

## Parameters

**directory** *path*

Specifies the path to the certificate.

**file** *filename*

Specifies the SSH public key with a .pub extension.

**host** *remote\_ip*

Specifies the IP address of the remote host.

**login** *login\_id*

Specifies the login name in the remote host.

**password** *password*

Specifies the password to access the remote host.

**user** *user\_acct*

Specifies the user name to access the remote host.

## Modes

Privileged EXEC mode

## Usage Guidelines

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

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

## Examples

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

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



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

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

The following commands demonstrate the use of special characters in a password.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# chassis

Sets the IPv4 or IPv6 address of a device chassis.

## Syntax

```
chassis { virtual-ip IPv4-address | virtual-ipv6 IPv6-address }  
no chassis
```

## Command Default

The default is the initial address of the device chassis.

## Parameters

**virtual-ip** *IPv4-address*

Sets an IPv4 address in dotted-decimal notation with a CIDR prefix (mask).

**virtual-ipv6** *IPv6-address*

Sets an IPv6 address in colon-separated hexadecimal notation with a CIDR prefix.

## Modes

Global configuration mode

## Usage Guidelines

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

Use this command to change the IP address to facilitate management, for example, if a device is moved to a different subnet. The IP address of the management platform should be in the same subnet as the devices it manages.

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

## Examples

IPv4:

```
device# configure terminal  
device(config)# chassis virtual-ip 10.11.12.13/20
```

IPv6:

```
device# configure terminal  
device(config)# chassis virtual-ipv6 2001:db8:8086:6502/64
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# cisco-interopability

Configures the device to interoperate with some legacy Cisco switches.

## Syntax

```
cisco-interopability { disable | enable }
```

## Command Default

Cisco interoperability is disabled.

## Parameters

### disable

Disables Cisco interoperability for the Multiple Spanning Tree Protocol (MSTP) device.

### enable

Enables Cisco interoperability for the MSTP enabled device.

## Modes

Protocol Spanning Tree MSTP mode

## Usage Guidelines

For some devices, the MSTP field, Version 3 Length, does not adhere to the current standards.

If Cisco interoperability is required on any device in the network, then all devices in the network must be compatible, and therefore enabled using this command for interoperability with a Cisco switch.

## Examples

To enable Cisco interoperability on a device:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# cisco-interopability enable
```

To disable Cisco interoperability on a device:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# cisco-interopability disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# class

Creates a class map in a policy map and enters the class map configuration mode.

## Syntax

**class** *class-mapname*

**no class** *class-mapname*

## Command Default

A policy map is not created.

## Parameters

*class-mapname*

The designated name for the class map.

## Modes

Global configuration mode

## Usage Guidelines

Use this command to configure a class map for a police policy map with QoS and policing parameters for inbound or outbound traffic. The class map must have been created and associated with match criteria using the **class-map** command. (Refer to the **qos cos** command.) When you launch the **class** command while in config-policy-map mode (refer to **policy-map**) for a policy, the system is placed in "configure policy-map classification" (config-policy-map-class) mode. Once this is done you can configure QoS and policing parameters for the class map using the commands for the specific parameters. The commands that set the parameters for a class map are:

- **conform-set-dscp**
- **conform-set-prec**
- **exceed-set-dscp**
- **exceed-set-prec**
- **police cir**
- **set-priority**

Each policy map can contain one class map.

Enter the **no policy-mapname** command to remove the policy map. Associate the policy map to the interface for inbound or outbound direction with the **service-policy** command (refer to **service-policy**).

Enter **no police** while in config-policy-map-class mode to remove all policing parameters for the class map.

Enter **no police** command followed by a policing parameter name to remove a specific parameter.

**NOTE**

The **cir** is mandatory for configuring a class map. Other parameters are optional. If optional parameters are not set then they will be treated as disabled. To delete the mandatory CIR parameter, you must delete all policer parameters while in the policy map class configuration mode using the **no police** command.

## Examples

This example configures a class-map called "default" within a policy-map.

```
device# configure terminal
device(config)# policy-map policymap1
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# class-map

Enters class (classification) map configuration mode.

## Syntax

```
class-map class-map-name
```

```
no class-map class-map-name
```

## Command Default

The class map name "default" is reserved and cannot be created by users.

## Parameters

*class-map-name*

Name of classification map. The map name is restricted to 64 characters.

## Modes

Global configuration mode.

## Usage Guidelines

Enter **no map class-map***class-map-name* while in global configuration mode to remove the classification map.

You can create up to 128 class maps.

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear arp

Clears some or all ARP caches.

## Syntax

```
clear arp [ ethernet slot / port | ip ip-address | ve ve_id ] [ no-refresh ] [ vrf vrf-name ]
```

## Parameters

### ethernet

Specifies a physical Ethernet interface.

#### slot

Specifies a valid slot number.

#### port

Specifies a valid port number.

### ip ip-address

Clears the ARP cache for a specified next-hop IP address.

### ve ve\_id

Specifies a virtual ethernet (VE) interface.

### no-refresh

Clears the ARP cache, without resending ARP requests to the local hosts.

### vrf vrf\_name

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

If the **no-refresh** keyword is not included, ARP requests are automatically triggered for the cleared entries. To avoid this triggering, include the **no-refresh** keyword.

## Examples

The following example clears all ARP entries on the device.

```
device# clear arp
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# clear counters

Clears the IP counter statistics on the switch.

## Syntax

```
clear counters [ access-list { ip | ipv6 | mac } [ all | interface { fcoe [ vn-number | all ] | port-channel number | slot-id number |  
vlan vlan_id } | storm-control ]
```

## Parameters

### access-list

Clears the IP counter statistics on all interfaces on the switch.

### all

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

### interface

Specifies an interface.

### port-channel number

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

### slot-id

Clears the IP counter statistics on a specified slot in the chassis.

### storm-control

Clears counters about traffic controlled by configured rate limits.

## Modes

Privileged EXEC mode

## clear counters access-list

For a given network protocol and inbound/outbound direction, clears ACL statistical information. You can clear all statistics for a specified ACL or only for that ACL on a specified interface. You can also clear statistical information for all ACLs bound to a specified Ethernet interface, VLAN, or VE.

### Syntax

```
clear counters access-list interface { ethernet slot / port | port-channel index | vlan vlan_id } { in | out }
clear counters access-list interface ve vlan_id { in | out }
clear counters access-list { ip | ipv6 } [ acl-name { in | out } ]
clear counters access-list { ip | ipv6 } acl-name interface { ethernet slot / port | port-channel index | ve vlan_id } { in | out }
clear counters access-list receive { ip | ipv6 }
clear counters access-list mac [ acl-name { in | out } ]
clear counters access-list mac acl-name interface { ethernet slot / port | port-channel index | vlan vlan_id } { in | out }
```

### Parameters

#### interface

Specifies an interface.

#### ethernet

Specifies a physical Ethernet interface.

*slot*

Specifies a valid slot number.

*port*

Specifies a valid port number.

#### port-channel *number*

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

#### in | out

Specifies the binding direction (incoming or outgoing).

#### vlan *vlan\_id*

(Available only on Layer 2) Specifies a VLAN.

#### ve *vlan\_id*

(Available only on Layer 3) Specifies a virtual Ethernet (VE) interface.

#### ip | ipv6 | mac

Specifies the network protocol.

#### receive

Specifies an ACL that applies to device receive-path traffic.

#### *acl-name*

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

## Modes

Privileged EXEC mode

## Examples

The following example clears ACL statistics on a specified Ethernet interface.

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

The following example clears ACL statistics for a specified MAC ACL on a specified Ethernet interface.

```
device# clear counters access-list mac MAC_ACL_1 interface ethernet 2/2
```

The following example clears ACL statistics for a specified MAC ACL on all interfaces on which this ACL is applied.

```
device# clear counters access-list mac MAC_ACL_1
```

The following example clears ACL statistics for a specified IPv4 ACL on a specified interface.

```
device# clear counters access-list ip IP_ACL_1 interface ethernet 2/3
```

The following example clears ACL statistics for a specified IPv4 ACL on all interfaces on which it is applied.

```
device# clear counters access-list ip IP_ACL_1
```

The following example clears incoming ACL statistics for a specified IPv6 ACL on a virtual Ethernet (VE) interface.

```
device# clear counters access-list ipv6 ip_acl_3 interface ve 10 in
```

The following example clears IPv6 receive-path ACL statistics.

```
device# clear counters access-list receive ipv6
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear counters access-list overlay type vxlan

Clears statistics of the specific overlay access list.

## Syntax

`clears counters access-list overlay type vxlan user-acl-name`

## Parameters

*user-acl-name*

The ACL name.

## Modes

Privileged EXEC mode.

## Examples

This example clears the statistics pertaining to the specified ACL.

```
device# clear counters access-list overlay type vxlan abc_ext
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear counters storm-control

Clears all broadcast, unknown unicast, and multicast (BUM) related counters in the system.

## Syntax

```
clear counters storm-control
```

```
clear counters storm-control [ broadcast | multicast | unknown-unicast ] [ interface ethernet slot/port ]
```

## Parameters

### broadcast

Clears all BUM-related counters in the system for the broadcast traffic type.

### multicast

Clears all BUM-related counters in the system for the multicast traffic type.

### unknown-unicast

Clears all BUM-related counters in the system for the unknown-unicast traffic type.

### interface ethernet slot/port

Clears all BUM-related counters in the system for the specified interface.

## Modes

Privileged EXEC mode.

## Usage Guidelines

This command clears the counters for broadcast, unknown-unicast, and multicast traffic for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interfaces.

## Examples

Clear counters for broadcast traffic on an Ethernet interface.

```
device# clear counters storm-control broadcast interface ethernet 4/1
```

Clear counters for all traffic types enabled on an Ethernet interface.

```
device# clear counters storm-control interface ethernet 4/1
```

Clear counters for all multicast traffic in the system.

```
device# clear counters storm-control multicast
```

Clear all BUM-related counters in the system.

```
device# clear counters storm-control
```

clear counters storm-control

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear dot1x statistics

Clears all accumulated dot1x port authentication statistics on the ports.

## Syntax

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

## Parameters

**interface ethernet slot/port**

Specifies to clear all dot1x statistics for a specified interface port.

## Modes

Privileged EXEC mode

## Examples

This example clears all accumulated dot1x port authentication statistics on all ports.

```
device# clear dot1x statistics
```

This example clears all dot1x statistics for a specified interface port.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip bgp dampening

Reactivates suppressed BGP4 routes.

## Syntax

```
clear ip bgp dampening [ ip-addr { / mask } ] [ vrf vrf-name ]
```

## Parameters

*ip-addr*

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

*mask*

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

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example unsuppresses all suppressed BGP4 routes.

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

This example unsuppresses suppressed BGP4 routes for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# clear ip bgp flap-statistics

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

## Syntax

```
clear ip bgp flap-statistics [ ip-addr { / mask } ] neighbor ip-addr | regular-expression string ] [ vrf vrf-name ]
```

## Parameters

*ip-addr*

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

*mask*

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

**neighbor**

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

*ip-addr*

IPv4 address of the neighbor.

**regular-expression**

Specifies a regular expression.

*string*

Regular expression.

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example clears the dampening statistics for a BGP4 route.

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

This example clears the dampening statistics for a BGP4 route for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip bgp local routes

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

## Syntax

```
clear ip bgp local routes [ vrf vrf-name ]
```

## Parameters

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example clears all BGP4 local routes.

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

This example clears BGP4 local routes for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip bgp neighbor

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

## Syntax

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

## Parameters

### all

Resets and clears all BGP4 connections to all neighbors.

### as-num

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

### peer-group-name

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

### ip-addr

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

### last-packet-with-error

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

### notification-errors

Clears all BGP4 connections identified as having notification errors.

### soft

Refreshes routes received from or sent to the neighbor.

#### in

Refreshes received routes.

#### prefix-filter

Refreshes Outbound Route Filters (ORFs) that are prefix-based.

#### out

Refreshes sent routes.

### soft-outbound

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

#### NOTE

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

### traffic

Clears the counters (resets them to 0) for BGP4 messages.

clear ip bgp neighbor

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example refreshes all BGP4 neighbor connections.

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

This example refreshes all BGP4 neighbor connections for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip bgp routes

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

## Syntax

```
clear ip bgp routes [ ip-addr [ / mask ] ] [ vrf vrf-name ]
```

## Parameters

*ip-addr*

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

*mask*

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

**vrf** *vrf-name*

Specifies the name of the VRF instance to associate with subsequent address-family configuration mode commands.

## Modes

Privileged EXEC mode

## Examples

This example clears all BGP4 routes.

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

This example clears BGP4 routes for VRF instance "red":

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip bgp traffic

Clears the BGP4 message counter for all neighbors.

## Syntax

```
clear ip bgp traffic [ vrf vrf-name ]
```

## Parameters

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example clears the BGP4 message counters.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip dhcp relay statistics

Clears IP DHCP Relay statistics.

## Syntax

```
clear ip dhcp relay statistics ip-address ip-address
```

## Command Default

DHCP relay statistics are present on the DHCP server.

## Parameters

**ip-address** *ip-address*

IPv4 address of DHCP server where client requests are to be forwarded.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to clear IP DHCP Relay statistics for a specific IP DHCP Relay address or all addresses on the device.

## Examples

The following example clears statistics for IP DHCP Relay

```
device# clear ip dhcp relay statistics ip-address 10.1.0.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip ospf

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

## Syntax

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

```
clear ip ospf counters { all | ethernet slot/port | loopback number | ve vlan_id } [ vrf vrf-name ]
```

```
clear ip ospf neighbor { ip-addr | all } [ vrf vrf-name ]
```

```
clear ip ospf routes { ip-addr/mask | all } [ vrf vrf-name ]
```

## Parameters

### all

Clears all OSPF data processes.

### vrf *name*

Specifies a VRF.

### counters

Clears OSPF counters.

#### all

Clears all counters.

#### ethernet *slot / port*

Specifies an Ethernet slot and port.

#### loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

#### ve *vlan\_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

### neighbor

Clears neighbors.

#### *ip-addr*

Specifies the IP address of the neighbor.

#### all

Clears all neighbors.

### routes

Clears matching routes or clears all routes.

#### *ip-addr/mask*

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

#### all

Clears all routes.



## Modes

Privileged EXEC mode

## Examples

The following example restarts the OSPF processes.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ip route

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

## Syntax

```
clear ip route { A.B.C.D | A.B.C.D/M } [ vrf vrf-name ]
```

```
clear ip route all [ vrf vrf-name ]
```

```
clear ip route slot line-card-number [ A.B.C.D | A.B.C.D/M ] [ vrf vrf-name ]
```

## Parameters

*A.B.C.D*

Specifies an IPv4 address.

*A.B.C.D/M*

Specifies an IPv4 address and mask.

vrf *vrf-name*

Specifies a VRF instance from which the user is currently retrieving routes.

all

Specifies all routes.

slot *line-card-number*

Specifies a line card.

## Modes

Privileged EXEC mode

## Examples

The following example clears the IP route specified by IP address 192.158.1.1/24.

```
device# clear ip route 192.158.1.1/24
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 bgp dampening

Reactivates suppressed BGP4 routes.

## Syntax

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

## Parameters

*ipv6-addr*

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

*mask*

IPv6 mask of a specified route in CIDR notation.

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example unsuppresses all suppressed BGP4+ routes.

```
device# clear ipv6 bgp dampening
```

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 bgp flap-statistics

Clears route-flap statistics for BGP4+ routes.

## Syntax

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

## Parameters

*ipv6-addr*

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

*mask*

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

**neighbor**

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

*ipv6-addr*

IPv6 address of the neighbor.

**regular-expression**

Specifies a regular expression.

*string*

Regular expression.

**vrf vrf-name**

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 bgp local routes

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

## Syntax

```
clear ipv6 bgp local routes [ vrf vrf-name ]
```

## Parameters

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example clears all BGP4+ local routes.

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

This example clears BGP4+ local routes for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 bgp neighbor

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

## Syntax

```
clear ipv6 bgp neighbor [ all | as-num | peer-group-name | ipv6-addr ] [ last-packet-with-error | notification-errors | soft [ in
[ prefix-filter ] | out ] | soft-outbound | traffic ] [ vrf vrfname ]
```

## Parameters

### all

Resets and clears all BGP4+ connections to all neighbors.

### as-num

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

### peer-group-name

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

### ipv6-addr

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

### last-packet-with-error

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

### notification-errors

Clears all BGP4+ connections identified as having notification errors.

### soft

Refreshes routes received from or sent to the neighbor.

#### in

Refreshes received routes.

#### prefix-filter

Refreshes Outbound Route Filters (ORFs) that are prefix-based.

#### out

Refreshes sent routes.

### soft-outbound

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

#### NOTE

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

### traffic

Clears the counters (resets them to 0) for BGP4+ messages.

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example refreshes all BGP4+ neighbor connections.

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

This example resets all the counters for BGP4+ messages.

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

This example clears BGP4+ connections with a specified peer group.

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 bgp routes

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

## Syntax

```
clear ipv6 bgp routes [ ipv6-addr [ / mask ] ] [ vrf vrfname ]
```

## Parameters

*ipv6-addr*

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

*mask*

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

**vrf** *vrf-name*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example clears specific BGP4+ routes.

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

This example clears specific BGP4+ routes for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# clear ipv6 bgp traffic

Clears the BGP4+ message counter for all neighbors.

## Syntax

```
clear ipv6 bgp traffic [ vrf vrf-name ]
```

## Modes

Privileged EXEC mode

## Parameters

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

## Examples

This example clears all BGP4+ message counters.

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

This example clears BGP4+ message counters for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 counters

Clears IPv6 counters on all interfaces or on a specified interface.

## Syntax

```
clear ipv6 counters [ all | interface { ethernet slot/port | loopback port-number | ve ve-id }
```

## Parameters

### all

Specifies all interfaces.

### ethernet

Represents a valid, physical Ethernet subtype.

#### slot

Specifies a valid slot number.

#### port

Specifies a valid port number.

### loopback

Specifies a loopback interface.

#### port-number

Port number of the loopback interface. The range is from 1 through 255.

### ve

Specifies a virtual Ethernet (VE) interface.

#### ve\_id

ID of the VE interface. The range is from 1 through 4096.

## Modes

Privileged EXEC mode

## Examples

The following example clears counters on Ethernet 2/3.

```
device# clear ipv6 counters interface ethernet 2/3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 dhcp relay statistics

Clears IPv6 DHCP Relay statistics

## Syntax

```
clear ipv6 dhcp relay statistics ip-address ip-address
```

## Command Default

DHCP relay statistics are present on the DHCP server.

## Parameters

**ip-address** *ip-addr*

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

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to clear all the DHCP Relay statistics.

## Examples

Clear all the DHCP Relay statistics on the device.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 neighbor

Removes entries from the IPv6 neighbor table.

## Syntax

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

## Parameters

### ipv6-address

Removes cache entries for the specified IPv6 address.

### force-delete

Force deletes all the dynamic neighbor entries.

### ethernet

Removes neighbor entries for the Ethernet interface.

### ve *ve-number*

Removes neighbor entries for the the specified Virtual Ethernet (VE) interface.

### no-refresh

Deletes all the dynamic neighbor entries.

### vrf *vrf-name*

Removes entries from the IPv6 neighbor table for the specified VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

You must specify the *ipv6-address* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373.

## Examples

The following example removes neighbor entries for Ethernet interface 1/3.

```
device# clear ipv6 neighbor ethernet 1/3 force-delete
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 ospf

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

## Syntax

```
clear ipv6 ospf all [ vrf vrf-name ]
clear ipv6 ospf counts [ vrf vrf-name ]
clear ipv6 ospf counts neighbor A.B.C.D [ vrf vrf-name ]
clear ipv6 ospf counts neighbor interface { ethernet slot/port | loopback number | ve vlan_id } [ A.B.C.D ]
clear ipv6 ospf { force-spf | redistribution | traffic } [ vrf vrf-name ]
clear ipv6 ospf neighbor A.B.C.D [ vrf vrf-name ]
clear ipv6 ospf neighbor all [ vrf vrf-name ]
clear ipv6 ospf neighbor interface { ethernet slot/port | loopback number | ve vlan_id } [ A.B.C.D ]
clear ipv6 ospf routes { IPv6addr | all } [ vrf vrf-name ]
```

## Command Default

Disabled.

## Parameters

**all**  
Clears all OSPFv3 data.

**counts**  
Clears OSPFv3 counters.

**neighbor**  
Clears all OSPF counters for a specified neighbor.  
*A.B.C.D*  
Specifies a neighbor.

**vrf vrf-name**  
Specifies a VRF.

**interface**  
Specifies an interface.

**ethernet slot / port**  
Specifies an Ethernet slot and port.

**loopback number**  
Specifies a loopback interface. Valid values range from 1 through 255.

**ve vlan\_id**  
Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

clear ipv6 ospf

**force-spf**

Performs the shortest path first (SPF) calculation without clearing the OSPFv3 database.

**redistribution**

Clears OSPFv3 redistributed routes.

**traffic**

Clears OSPFv3 traffic statistics.

**routes**

Clears OSPFv3 routes.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use the **force-spf** keyword to perform the shortest path first (SPF) calculation without clearing the OSPFv3 database.

## Examples

The following example restarts the OSPFv3 processes.

```
device# clear ipv6 ospf all
```

The following example clears all OSPFv3 counters for a specified neighbor.

```
device# clear ipv6 ospf counts neighbor 10.10.10.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 route

Clears IPv6 routes.

## Syntax

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

## Parameters

*ipv6-address*

Removes IPv6 routes for the specified IPv6 address.

**vrf** *vrf-name*

Removes IPv6 routes for the specified VPN Routing and Forwarding (VRF) instance.

**all**

Removes all IPv6 routes.

**slot** *slot-number*

Removes IPv6 routes for the specified line card.

## Modes

Privileged EXEC mode

## Examples

The following example clears IPv6 routes associated with the prefix 2000:7838::/32.

```
device# clear ipv6 route 2000:7838::/32
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear ipv6 vrrp statistics

Clears IPv6 VRRPv3 session statistics for all virtual groups, for a specified interface, or for a specified virtual group.

## Syntax

```
clear ipv6 vrrp statistics [ all ]
```

```
clear ipv6 vrrp statistics [ interface { ethernet slot/port | ve vlan_id } ]
```

```
clear ipv6 vrrp statistics [ session VRID ]
```

## Parameters

### all

Clears all IPv6 VRRP statistics.

### session *VRID*

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

### interface

Specifies an interface.

### ethernet *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

### ve *vlan\_id*

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

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is supported in IPv6 VRRPv3 and VRRP-E-v3.

## Examples

The following example clears all IPv6 VRRPv3 statistics for all virtual groups.

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

The following example clears statistics for an IPv6 VRRPv3 session of virtual group 25.

```
device# clear ipv6 vrrp statistics session 25
```

The following example clears IPv6 VRRPv3 statistics on a specified virtual Ethernet interface.

```
device# clear ipv6 vrrp statistics interface ve 10
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis all

Clears all IS-IS information.

## Syntax

`clear isis all`

## Modes

Privileged EXEC mode

## Examples

This example clears all IS-IS information for a device.

```
device# clear isis all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis counts

Clears IS-IS error statistics for a device.

## Syntax

```
clear isis counts
```

## Modes

Privileged EXEC mode

## Examples

This example clears IS-IS error statistics.

```
device# clear isis counts
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis database

Clears IS-IS database entries.

## Syntax

```
clear isis database [ lsp-id level-1 | level-2 ]
```

## Parameters

### **lsp-id**

Specifies a link-state packet (LSP) in HHHH.HHHH.HHHH.HH-HH format or by entering a name, HH-HH.

### **level-1**

Specifies Level 1 packets only.

### **level-2**

Specifies Level 2 packets only.

## Modes

Privileged EXEC mode

## Examples

This example clears IS-IS database entries, specifying a LSP name of "XMR.00-00".

```
device# clear isis database XMR-1.00-00
```

This example clears IS-IS database entries for Level 1 LSPs.

```
device# clear isis database level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis force-spf

Performs the shortest path first (SPF) calculation without clearing the IS-IS database.

## Syntax

```
clear isis force-spf [ level-1 | level-2 ]
```

## Parameters

### level-1

Specifies Level 1 packets only.

### level-2

Specifies Level 2 packets only.

## Modes

Privileged EXEC mode

## Examples

This example specifies that SPF calculations can be performed without clearing the IS-IS database for Level 2 packets.

```
device# clear isis force-spf level-2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis force-v6spf

Performs the IPv6 shortest path first (SPF) calculation without clearing the IS-IS database.

## Syntax

```
clear isis force-v6spf [ level-1 | level-2 ]
```

## Parameters

### level-1

Specifies Level 1 packets only.

### level-2

Specifies Level 2 packets only.

## Modes

Privileged EXEC mode

## Examples

This example specifies that IPv6 SPF calculations can be performed without clearing the IS-IS database for Level 1 packets.

```
device# clear isis force-v6spf level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis ipv6 spf-log

Clears IPv6 IS-IS SPF logs.

## Syntax

```
clear isis ipv6 spf-log [ level-1 | level-2 ]
```

## Parameters

### level-1

Specifies Level 1 packets only.

### level-2

Specifies Level 2 packets only.

## Modes

Privileged EXEC mode

## Examples

This example clears IPv6 IS-IS logs for Level 1 packets.

```
device# clear isis ipv6 spf-log level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis neighbor

Clears IS-IS neighbors.

## Syntax

```
clear isis neighbor { lsp-id | all } [ ethernet slot/port | ve vlan_id ]
```

## Parameters

### **lsp-id**

Specifies a link-state packet (LSP) n HHHH.HHHH.HHHH.HH-HH format or by entering a name, HH-HH.

### **all**

Specifies all neighbors.

### **ethernet slot / port**

Specifies an Ethernet slot and port.

### **ve vlan\_id**

Specifies a virtual Ethernet (VE) interface.

## Modes

Privileged EXEC mode

## Examples

This example clears IS-IS neighbors, specifying a LSP name of "XMR.00-00".

```
device# clear isis neighbor XMR-1.00-00
```

This example clears all IS-IS connections for a specified Ethernet interface.

```
device# clear isis neighbor all ethernet 1/1
```

This example refreshes all IS-IS neighbors.

```
device# clear isis neighbor all
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# clear isis route

Clears IS-IS routes.

## Syntax

```
clear isis route { ip-address | ip-address/mask | all }
```

## Parameters

*ip-address*

Clears all routes that match the prefix that you specify.

*ip-address/mask*

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

**all**

Specifies all routes.

## Modes

Privileged EXEC mode

## Examples

This example clears IS-IS routes that match the IP address 10.1.1.1.

```
device# clear isis route 10.1.1.1
```

This example clears all IS-IS routes.

```
device# clear isis route all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis spf-log

Clears IPv4 IS-IS SPF logs.

## Syntax

```
clear isis spf-log [ level-1 | level-2 ]
```

## Parameters

### level-1

Specifies Level 1 packets only.

### level-2

Specifies Level 2 packets only.

## Modes

Privileged EXEC mode

## Examples

This example clears IPv4 IS-IS logs for Level 2 packets.

```
device# clear isis spf-log level-2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear isis traffic

Clears IS-IS packet counters.

## Syntax

```
clear isis traffic
```

## Modes

Privileged EXEC mode

## Examples

This example clears IS-IS packet counters.

```
device# clear isis traffic
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear lldp neighbors

Clears the Link Layer Discovery Protocol (LLDP) neighbor information on all or specified ethernet interfaces.

## Syntax

```
clear lldp neighbors [ interface ethernet slot/port ]
```

## Parameters

### ethernet

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

### slot

Specifies a valid slot number.

### port

Specifies a valid port number.

## Modes

Privileged EXEC mode

## Usage Guidelines

If the **interface** parameter is not specified, this command clears the LLDP neighbor information received on all the interfaces.

## Examples

To clear the LLDP neighbor information for all interfaces:

```
device# clear lldp neighbors
```

To clear LLDP neighbor information on a specific ethernet interface:

```
device# clear lldp neighbors interface ?
Possible completions:
ethernet Ethernet interface
device# clear lldp neighbors interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
 1/1
 1/2
 1/3
 1/4
 1/5
 1/6
 1/8
 1/9
 1/10
 1/11
 1/12
 1/13
 1/14
 1/15
 1/16
 1/17
 1/18
 1/19
 1/20
 1/21
 1/22
 1/23
 1/24
 1/25
 1/29
 1/30
 1/31
device# clear lldp neighbors interface ethernet 1/24
device#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear lldp statistics

Clears LLDP statistics for all interfaces or a specified Ethernet interface.

## Syntax

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

## Parameters

### **ethernet**

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

### *slot*

Specifies a valid slot number.

### *port*

Specifies a valid port number.

## Modes

Privileged EXEC mode

## Usage Guidelines

If the **interface** parameter is not specified, this command clears all the LLDP statistics on all interfaces.

## Examples

To clear all the LLDP statistics for all interfaces:

```
device# clear lldp statistics
```

To clear LLDP neighbor information on a specific ethernet interface:

```

device# clear lldp statistics interface ?
Possible completions:
ethernet  Ethernet interface
device# clear lldp statistics interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
 1/1
 1/2
 1/3
 1/4
 1/5
 1/6
 1/8
 1/9
 1/10
 1/11
 1/12
 1/13
 1/14
 1/15
 1/16
 1/17
 1/18
 1/19
 1/20
 1/21
 1/22
 1/23
device#clear lldp statistics interface ethernet 1/23
device#

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear mac-address-table

Removes interface entries from the MAC address table.

## Syntax

```
clear mac-address-table cluster cluster-id [client [client-id]] | dynamic [address mac-address | bridge-domain [id] | interface
ethernet slot/port | port-channel number | logical-interface ethernet slot/port [:brk-out], lif-id | vlan vlan-id]
```

## Parameters

### bridge-domain

Specifies clearing MAC addresses learned under a bridge domain.

*id*

Specifies a bridge-domain identifier.

### cluster *cluster-id*

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

### client *client-id*

Specifies clearing the client instance. Specify the client ID with a maximum of 64 characters.

### dynamic address *MAC-address*

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

### interface ethernet *slot/port*

Specifies clearing the ethernet interface with a valid slot number/port number.

### port-channel *number*

Specifies clearing the port channel interface number. The range is from 1 - 512 based on the platform.

### logical-interface ethernet *slot/port* [:*brk-out*], *lif-id*

Specifies clearing the logical ethernet interface on a specified slot/port number. The breakout interface option can be used with the LIF ID.

### vlan *vlan id*

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

## Modes

Privileged EXEC mode.

## Usage Guidelines

When a bridge-domain identifier is not specified, MAC addresses learned under all bridge domains are removed from the MAC address table. If a specific address is not specified, all dynamic mac-addresses are deleted from the MAC address table.



## Examples

The following example shows how to clear MAC addresses learned under bridge domain 1 from the MAC address table.

```
device# clear mac-address-table dynamic bridge-domain 1
```

The following example shows how to clear MAC addresses learned from vlan 1 from the MAC address table.

```
device# clear mac-address-table dynamic vlan 1
```

The following example shows how to clear MAC addresses from a logical interface ethernet 3/10 LIF breakout interface.

```
device# clear mac-address-table dynamic 3/10:5.200
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear mpls auto-bandwidth-samples

Deletes the sample-history from the auto-bandwidth LSPs.

## Syntax

```
clear mpls auto-bandwidth-samples [ lsp lsp_name ]
```

## Command Default

None.

## Parameters

**lsp** *lsp\_name*

The **lsp** option clears the auto-bandwidth sample history for the LSP specified through the *lsp\_name*.

## Modes

EXEC mode.

## Examples

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear mpls lsp

Allows the user to reset normal LSPs. The user has the option of supplying the primary or secondary parameter for a normal LSP to reset only the primary or secondary path of the LSP.

## Syntax

```
clear mpls lsp { lsp_name } [ primary | secondary ]
```

## Command Default

None.

## Parameters

*lsp\_name*

Specifies the target LSP by name.

**primary**

Specifies that the primary LSP path associated with the *lsp\_name* is reset and restarted.

**secondary**

Specifies that the secondary LSP path associated with the *lsp\_name* is reset and restarted.

## Modes

Privileged EXEC mode.

## Examples

When the user resets an LSP with the clear mpls lsp command, the following information message is displayed.

```
"Disconnecting signaled LSP name"  
"Connecting signaled LSP name"
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear mpls statistics

Clears the MPLS statistics.

## Syntax

```
clear mpls statistics { oam }
```

```
clear mpls statistics { transit [ label label | ldp [ ip_addr | submask | label ] | rsvp label ] }
```

```
clear mpls statistics { tunnel [ destination ip_addr | index vif_index | ldp [ destination ip_addr | index vif_index ] | rsvp [ destination ip_addr | index vif_index | name name ] ] }
```

## Parameters

### oam

Clears the MPLS OAM statistics.

### transit

Clears the MPLS transit statistics.

#### label *label*

Clears the MPLS transit statistics for the selected label.

#### ldp *ip\_addr*

Clears the MPLS transit LDP statistics for the selected IP address.

#### rsvp

Clears the MPLS transit RSVP statistics .

### tunnel

Clears the MPLS tunnel statistics.

#### destination *destination*

Clears the MPLS tunnel statistics for the selected tunnel destination.

#### index *vif\_index*

Clears the MPLS tunnel statistics for the selected tunnel index.

#### ldp

Clears the MPLS tunnel LDP statistics.

#### destination *destination*

Clears the MPLS tunnel statistics for the selected tunnel destination.

#### index *vif\_index*

Clears the MPLS tunnel statistics for the selected tunnel index.

#### rsvp

Clears the MPLS tunnel RSVP statistics.

#### destination *destination*

Clears the MPLS tunnel statistics for the selected tunnel destination.

#### index *vif\_index*

Clears the MPLS tunnel statistics for the selected tunnel index.

**name** *name*

Clears the MPLS tunnel statistics for the selected named tunnel.

## Modes

MPLS policy mode.

## Examples

The following example clears the MPLS statistics.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-mpls-policy)# clear mpls statistics
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# clear openflow

Clears a single OpenFlow rule based on a Flow ID or deletes all flows/groups/meters configured in the system.

## Syntax

```
clear openflow all | flowid flowid
```

## Parameters

**all**

Deletes all flows in the flow table.

**flowid** *flowid*

Deletes a single OpenFlow rule with the specified Flow ID.

## Modes

Privileged EXEC mode

## Usage Guidelines

## Examples

To delete a single OpenFlow rule based on a Flow ID:

```
device# clear openflow flowid 255
```

To delete all flows/groups/meters configured in the system:

```
device# clear openflow all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear policy-map-counters

Provides a mechanism for clearing the policy map counters.

## Syntax

```
clear policy-map-counters [ interface ethernet slot/port ] [ in | out ]
```

## Parameters

### interface

Specifies an interface.

### ethernet

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

### slot/port

Specifies a slot and port number.

### in

Specifies clearing the ingress counters.

### out

Specifies clearing the egress counters.

## Modes

Privileged EXEC mode

## Usage Guidelines

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear statistics bridge-domain

Clears the statistics for all the logical interfaces on bridge domains.

## Syntax

```
clear statistics bridge-domain bd-id
```

## Parameters

*bd-id*

The bridge domain ID.

## Command Default

Statistics are disabled.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is also available in global configuration mode.

The **clear statistics bridge-domain** *bd-id* command clears the statistics for all the logical interfaces on a specific bridge domain.

## Examples

The following example shows how to clear the statistics for all the logical interfaces on all bridge domains.

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

The following example shows how to clear the statistics for all the logical interfaces on bridge domain 2.

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

## History

Release version	Command history
16r.1.01	This command was introduced.



# clear statistics openflow

Clears the flow statistics for all flows or for a specified flow.

## Syntax

```
clear statistics openflow [controller | flow | group | meter]
```

## Parameters

*controller*

Sends statistics for the controller in a flow.

*flow*

Deletes the flow statistics for a specified flow on the OpenFlow controller.

*group*

Clears statistics for all groups.

*meter*

Clears statistics for all meters.

## Modes

Privileged EXEC mode

## Examples

```
device# clear statistics openflow
controller  send to controller statistics
flow       Flow
group      Clear statistics for all groups
meter     Clear statistics for all meters
device#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear statistics vlan

Clears the statistics for all the ports and port channels on configured VLANs.

## Syntax

```
clear statistics vlan vlan-id
```

## Parameters

*vlan-id*

The specific VLAN ID.

## Command Default

Statistics are disabled.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is also available in global configuration mode.

The **clear statistics vlan** *vlan-id* command clears the statistics for all the ports and port channels on the given VLAN.

## Examples

The following example shows how to clear the statistics for all the ports and port channels on the given VLAN.

```
device# clear statistics vlan
```

The following example shows how to clear the statistics for all the ports and port channels on VLAN 10.

```
device# clear statistics vlan 10
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# clear tm voq-stat ingress-device

Clears the traffic management VOQ statistics on the ingress device for a specified ethernet port, or for all ports.

## Syntax

```
clear tm voq-stat ingress-device {{ ethernet slot/port } {egress-port ethernet slot/port} | all }
```

```
clear tm voq-stat ingress-device all egress-port ethernet slot/port | all
```

## Parameters

**ethernet slot/port**

Specifies the ethernet interface in slot/port format.

**egress-port ethernet slot/port**

Specifies clearing the traffic management statistics on the egress ethernet slot/ port.

**all**

Specifies clearing the traffic management statistics for all ports.

## Modes

Privileged EXEC mode.

## Examples

To clear VOQ statistics information on the egress-port for ethernet 1/1, use the following command.

```
device# clear tm voq-stat ingress-device ethernet 1/1 egress-port ethernet 1/1
```

To clear all VOQ statistics information on the egress-port for ethernet 1/1, use the following command.

```
device# clear tm voq-stat ingress-device all egress-port ethernet 1/1
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# clear tm voq-stat slot

Clears the traffic management VOQ statistics for a line card (LC) in a named slot.

## Syntax

```
clear tm voq-stat slot slot_number [ cpu-group [ cpu_group_id | all ]
```

## Parameters

*slot\_number*

The linecard slot.

**cpu-group** *cpu\_group\_id*

The ID number for the CPU group.

## Modes

Privileged EXEC mode.

## Examples

To clear information about the VOQ for the LC in slot 1 CPU group 1 use the following command.

```
device# clear tm voq-stat slot 1 cpu-group 1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear tunnel statistics

Clears statistics from the tunnel interfaces.

## Syntax

```
clear tunnel statistics tunnel-id
```

## Parameters

*tunnel-id*

Specifies the tunnel ID.

## Modes

Privileged EXEC mode

## Examples

This example removes statistics from a tunnel interface.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear vrrp statistics

Clears VRRP statistics.

## Syntax

```
clear vrrp statistics
```

```
clear vrrp statistics [ interface { ethernet slot/port | ve vlan_id } ]
```

```
clear vrrp statistics session VRID
```

## Parameters

**interface**

Specifies an interface.

**ethernet** *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

**ve** *vlan\_id*

Specifies the VE VLAN number. The range is from 1 through 6144.

**session** *VRID*

Specifies the virtual group ID on which to clear statistics. The range is from 1 through 255.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command clears VRRP session statistics for all virtual groups, for a specified interface or for a specified virtual group.

This command is for VRRP and VRRP-E. VRRP-E supports only the **ve** *vlan\_id* interface type.

To clear all vrrp statistics, use the **clear vrrp statistics** command with no operands.

## Examples

The following example clears all VRRP statistics for all virtual groups.

```
device# clear vrrp statistics
```

The following example clears statistics for Ethernet interface 1/6.

```
device# clear vrrp statistics interface ethernet 1/6
```

The following example clears statistics for a session for a VRRP virtual group called "vrrp-group-25".

```
device# clear vrrp statistics session 25
```

The following example clears VRRP statistics on a specified virtual Ethernet (VE) interface.

```
device# clear vrrp statistics interface ve 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# CLI

In a Python shell, runs a device CLI command or series of commands. You can also assign the output of such commands to a Python object.

## Syntax

```
CLI ( ' device-CLI-command ' [ \n ' device-CLI-command ' ] [ do_print = ] { True | False } )
```

## Parameters

*device-CLI-command*

An SLX-OS CLI command. You separate additional commands with `\n`.

**do\_print =**

Specify whether or not to print the output of *device-CLI-command* to the default device. The default is to print the output.

**True**

Print the output.

**False**

Do not print the output.

## Modes

Python command shell

## Usage Guidelines

Divergences between the CLI syntax and Python syntax include the following differences:

- Although in general, the CLI syntax is not case-sensitive, our convention is to use lower-case.
- Python syntax is case sensitive. Regarding the syntax documented in the current topic, note the following:
  - The syntax of the command is upper case (CLI) and not lower case (cli).
  - The syntax of the **do\_print =** options is to capitalize the first letter: { **True** | **False** }

In Python, double quotes (") and single quotes (') are equivalent.

As delimiter between multiple CLI commands, use `\n`.

There is a difference between running a sequence of SLX-OS CLI commands in the Python shell rather than in the standard SLX-OS interface. Whereas in the standard interface the result of a command is persistent, in the Python shell each `CLI ( )` statement is independent of any preceding ones.

For support of the `CLI ( )` command, although a Python script must include a `from CLI import CLI` statement, this statement is automatically implemented when launching the Python interpreter interactively.



Within a script or interactive session, if you assign a CLI command or series of commands to a Python variable, you can then append the following functions to the variable:

- **.rerun()**—updates the variable from a new run of the CLI command or series of commands.

```
device# python
Python 3.4.3 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_running_ve = CLI('show running-config interface ve')
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

% No entries found.
# The SLX-OS show running-config interface ve command is run,
# and that command is assigned to the Python variable cmd_show_running_ve.

>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
# A series of three commands are run and assigned to the Python variable cmd_config_ve.
!Command: configure
interface ve 101-103
!Time: Mon Aug 22 16:53:13 2016

>>> cmd_show_running_ve.rerun()
# The rerun() function appended to cmd_show_running_ve gives the following output:
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

interface Ve 101
shutdown
!
interface Ve 102
shutdown
!
interface Ve 103
shutdown
!
!
```

- **.get\_output()**—returns the value of a new run of the CLI command or series of commands, as a list.

```
#Required in all scripts for SLX:
from CLI import CLI
# Import the Python Regular Expressions (re) module:
import re
# Create Python objects:
slot_firmware = {}

cmd_show_ver = CLI("show ver", False)
# Using .get_output(), assign the result of show ver to a Python object named output:
output = cmd_show_ver.get_output()
for line in output:
    found = re.search(r'^(\S+)\s+(\S+)\s+(\S+)\s+ACTIVE.*$', line, re.M)
    if found:
        slot_firmware[found.group(1)] = found.group(3)

print("SLOT_FIRMWARE:\n")
for key in slot_firmware:
    print("\t", key, "\t=> ", slot_firmware[key])
```

## Examples

The following example launches the Python shell and then both assigns a series of CLI configuration commands to a Python variable and runs those commands.

```
device# python
Python 3.4.3 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
!Command: configure
      interface ve 101-103
!Time: Mon Aug 22 16:57:36 2016
>>>
```

The following example launches the Python shell and then both assigns a CLI operational command to a Python variable and runs that command.

```
device# python
Python 3.4.3 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_reload_system = CLI('reload system \n y')
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# client

Configures a Multi-Chassis Trunking (MCT) client for a cluster and access cluster client configuration mode.

## Syntax

**client** *client-name client-id*

**no client** *client-name client-id*

## Parameters

*client-name*

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

*client-id*

Specifies the cluster client ID. The ID value range can be from 1 through 512.

## Modes

Cluster client configuration mode

## Usage Guidelines

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

## Examples

The following example configures a cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)#
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# client-interface

Configures a CEP or CCEP interface to the cluster client instance.

## Syntax

```
client-interface { ethernet slot/port | port-channel number }
no client-interface
```

## Parameters

**ethernet** *slot/port*

Configures the specified Ethernet port as the client CEP or CCEP.

**port-channel** *number*

Configures the specified port channel as the client CEP or CCEP. The port channel *number* specifies the LAG ID.

## Modes

Cluster client configuration mode

## Usage Guidelines

The **no** form of the command removes the client interface.

The same client interface cannot be added under multiple client entries.

A client interface is not allowed to be updated when the client is in deploy state. It needs to be removed first before adding a new interface.

## Examples

The following example shows how to configure a client interface.

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

## History

Release version	Command history
16r.1.01	This command was introduced.

# client-interfaces-shutdown

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

## Syntax

```
client-interfaces shutdown
```

```
no client-interfaces shutdown
```

## Modes

Cluster configuration mode

## Usage Guidelines

The **no** form of the command reenables the local client interfaces.

## Examples

The following example shows the disabling of all the client interfaces in the cluster.

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

## History

Release version	Command history
16r.1.01	This command was introduced.

# client-isolation-strict

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

## Syntax

```
client-isolation-strict
no client-isolation-strict
```

## Command Default

Client-isolation mode is based on the peer IP address. The node with the lower peer IP address is set to the client-isolation mode of loose, while the node with the higher peer IP address is set to the client-isolation mode of strict.

## Modes

Cluster configuration mode

## Usage Guidelines

In strict mode, when the EVPN control session goes down, the interfaces on both the cluster devices are administratively shut down. In strict mode, the client is completely isolated from the network if the control session is not operational.

In loose mode, when the EVPN control session goes down, the peer device performs the master/slave negotiation. After negotiation, the slave shuts down its peer ports, and the master peer ports continue to forward the traffic (keep-alive VLAN configured).

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

### NOTE

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

The **no** form of the command resets the default client isolation mode behavior based on the peer IP address.

## Examples

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

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

## History

Release version	Command history
16r.1.01	This command was introduced.

# client-to-client-reflection

Enables routes from one Route Reflector (RR) client to be reflected to other clients by the host device on which it is configured.

## Syntax

`client-to-client-reflection`

`no client-to-client-reflection`

## Command Default

Enabled.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

## Usage Guidelines

When this command is used, the host device on which it is configured becomes the route-reflector server.

The **no** form of the command disables route reflection between clients.

## Examples

The following example configures client-to-client reflection on the BGP host device for the IPv4 unicast address-family.

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

The following example disables client-to-client reflection on the BGP host device for the IPv6 unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# no client-to-client-reflection
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# cluster

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

## Syntax

```
cluster cluster-name cluster-id
```

```
no cluster cluster-name cluster-id
```

## Parameters

*cluster-name*

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

*cluster-id*

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

## Modes

Global configuration mode

## Usage Guidelines

### NOTE

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

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

## Examples

The following example configures an MCT cluster.

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

## History

Release version	Command history
16r.1.01	This command was introduced.



# cluster-id

Configures a cluster ID for the route reflector.

## Syntax

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

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

## Command Default

The default cluster ID is the device ID.

## Parameters

*num*

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

*ip-addr*

IPv4 address in dotted-decimal notation.

## Modes

BGP configuration mode

## Usage Guidelines

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

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

## Examples

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# compare-med-empty-aspath

Enables comparison of Multi-Exit Discriminators (MEDs) for internal routes that originate within the local autonomous system (AS) or confederation

## Syntax

```
compare-med-empty-aspath
no compare-med-empty-aspath
```

## Command Default

Disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

The following example configures the device to compare MEDs.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# compare-routerid

Enables comparison of device IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

## Syntax

```
compare-routerid
no compare-routerid
```

## Command Default

This feature is disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

This example configures the device always to compare device IDs.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# confederation identifier

Configures a BGP confederation identifier.

## Syntax

**confederation identifier** *autonomous-system number*  
**no confederation identifier**

## Command Default

No BGP confederation identifier is identified.

## Parameters

*autonomous-system number*

Specifies an autonomous system number (ASN). The configurable range of values is from 1 through 4294967295.

## Modes

BGP configuration mode

## Usage Guidelines

Use the **no** form of this command to remove a BGP confederation identifier.

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

## Examples

This example specifies that confederation 65220 belongs to autonomous system 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65220
device(config-bgp-router)# confederation identifier 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# confederation peers

Configures subautonomous systems to belong to a single confederation.

## Syntax

**confederation peers** *autonomous-system number* [ ...*autonomous-system number* ]  
**no confederation peers**

## Command Default

No BGP peers are configured to be members of a BGP confederation.

## Parameters

*autonomous-system number*

Autonomous system (AS) numbers for BGP peers that will belong to the confederation. The configurable range of values is from 1 through 4294967295.

## Modes

BGP configuration mode

## Usage Guidelines

Use the **no** form of this command to remove an autonomous system from the confederation.

## Examples

This example configures autonomous systems 65520, 65521, and 65522 to belong to a single confederation under the identifier 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65020
device(config-bgp-router)# confederation identifier 100
device(config-bgp-router)# confederation peers 65520 65521 65522
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# configure terminal

Enters global configuration mode.

## Syntax

`configure terminal`

## Modes

Privileged EXEC mode

# conform-set-dscp

Configures the packet DSCP priority of a class map.

## Syntax

`conform-set-dscp dscp-num`

`no conform-set-dscp dscp-num`

## Parameters

*dscp-num*

Specifies that traffic with bandwidth requirements within the rate configured for CIR that has the packet DSCP priority set to the value specified by the *dscp-num* variable. Valid values are 0 through 63.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** version of this command to remove the parameter from the class map.

## Examples

Example of setting this parameter.

```
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
device(config-policymap-class-police)# conform-set-dscp 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# conform-set-prec

Configures the packet IP precedence value of a class map.

## Syntax

`conform-set-prec prec-num`

## Parameters

*prec-num*

Specifies that traffic with bandwidth requirements within the rate configured for CIR will have packet IP precedence value (first 3 bits of DSCP) set to the value in the *prec-num* variable. Valid values are 0 through 7.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** version of this command to remove the parameter from the class map.

## Examples

Example of setting this parameter.

```
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
device(config-policymap-class-police)# conform-set-prec 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# conform-set-tc

Configures the CIR internal queue assignment of a class map.

## Syntax

`conform-set-tc trafficclass`

`no conform-set-tc trafficclass`

## Parameters

*trafficclass*

Specifies that traffic with bandwidth requirements within the rate configured for CIR has the traffic class (internal queue assignment) set to the configured value. Valid values are 0 through 7.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete parameters for a class map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** version of this command to remove the parameter from the class map.

## Examples

Example of setting this parameter.

```
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
device(config-policymap-class-police)# conform-set-tc 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# connector

Accesses connector configuration mode for the 40G port on the SLX 9850 36X100G line card (LC).

## Syntax

`connector slot/port`

## Parameters

*slot/port*

Specifies a valid slot and port number on the line card.

## Modes

Hardware configuration mode

## Usage Guidelines

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

Power off the line card before using this command.

## Examples

The following example shows the accessing of the connector configuration mode for a 40G port on the 36X100G LC.

```
device# power-off linecard 4
device# configure terminal
device(config)# hardware
device(config-hardware)# connector 4/2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# copy

Copies configuration data.

## Syntax

```
copy source_file destination_file
```

## Parameters

*source\_file*

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

**default-config**

The default configuration.

**running-config**

The running configuration.

**startup-config**

The startup configuration.

**flash://filename**

A file in the local flash memory.

**ftp://username:password@host\_ip\_address/path**

A file on a remote host. Transfer protocol is FTP.

**scp://username:password@host\_ip\_address/path**

A file on a remote host. Transfer protocol is SCP.

**sftp://username:password@host\_ip\_address/path**

A file on a remote host. Transfer protocol is SFTP.

**tftp://username:password@host\_ip\_address/path**

A file on a remote host. Transfer protocol is TFTP.

**usb://path**

A file on an attached USB device.

*destination\_file*

The destination file. Specify one of the following parameters:

**default-config**

The default configuration.

**running-config**

The running configuration.

**startup-config**

The startup configuration.

**flash://filename**

A file in the local flash memory.

**ftp://username:password@host\_ip\_address//path**

A file on a remote host. Transfer protocol is FTP.

**scp://username:password@host\_ip\_address//path**  
A file on a remote host. Transfer protocol is SCP.

**sftp://username:password@host\_ip\_address/path**  
A file on a remote host. Transfer protocol is SFTP.

**tftp://username:password@host\_ip\_address/path**  
A file on a remote host. Transfer protocol is TFTP.

**usb://path**  
A file on an attached USB device.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to back up and restore configuration files with various protocols.

This command is supported only on the local switch.

IPv4 and IPv6 addresses are supported.

The special characters of dollar sign "\$" and exclamation point "!" can be used as part of the password variable, provided they are paired with the correct escape characters. The "\$" must be paired with two backslashes "\". For example, if your password choice was "\$password" on a remote server, you must use "username:\\\$password@1.1.1.1" for the **copy** command. The exclamation point must be paired with a single backslash in the **copy** command, such as "username:\\!password@1.1.1.1".

## Examples

To save the running configuration to a file:

```
device# copy running-config flash://myconfig
```

To overwrite the startup configuration with a locally saved configuration file:

```
device# copy flash://myconfig running-config
```

To overwrite the startup configuration with a remotely archived configuration file:

```
device# copy scp://user:password@10.10.10.10//myconfig startup-config
```

To overwrite the startup configuration with a configuration file saved on an attached USB device:

```
device# copy usb://myconfig startup-config
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## COS

Configures the a Class of Service (CoS) priority value for all packets traveling through the LSP.

## Syntax

`cos number`

`no cos number`

## Parameters

*number*

Specifies the CoS priority value. Enter a number from 0 to 7. The lowest priority is 0, the default value. The highest priority is 7.

## Modes

MPLS LSP configuration mode

## Usage Guidelines

The 3-bit EXP field in the MPLS header defines a CoS value for packets traveling through the LSP. When you set the CoS value, it is applied to the EXP field in the MPLS header of all packets entering this LSP. Then, all packets traveling through an LSP have the same priority as they travel the MPLS domain.

The MPLS CoS value determines the priority within an MPLS domain only. When the label is popped, the CoS value in the MPLS header is discarded and it is not copied back to the IP ToS field.

Use the **no** form of the command to remove the configured setting.

## Examples

The following example configures the CoS priority of 7 to all packets traveling through the tunnel4 LSP.

```
device(config-router-mpls)# lsp tunnel4
device(config-router-mpls-lsp-tunnel4)# cos 7
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# crypto ca authenticate

Downloads the CA certificate from the remote certificate server for the trust point.

## Syntax

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

```
no crypto ca authenticate { trustpointCA_name}
```

## Parameters

*trustpointCA\_name* *trustpointCA\_name*

Defines the name of the trust point you are authenticating. This name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

**directory** *remote\_dir\_name*

Defines the directory where the certification file resides.

**file** *cert\_file*

Defines the name of the certification file.

**host** *host\_address*

Defines the host name or IP address of the remote certificate server.

**protocol** {FTP | SCP}

Specifies the use of either FTP or SCP protocol for accessing the certification file.

**user** *host\_login*

Defines user name for the host server.

**password** *host\_user\_password*

Defines the password for the user name on the host server.

### NOTE

It is recommended to not list the password in command line for security purposes; the user will be prompted for the password.

## Modes

Privileged EXEC mode

## Usage Guidelines

This is the CA certificate of the Trusted CA that you want to sign the CSR and generate the identity certificate.

The *trustpoint\_CAname* name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command.

Use the no form of the command to delete the certificate.

## Examples

Typical command example.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# crypto ca enroll

Enrolls the trust point by generating the Certificate Signing Request (CSR) and exporting it to the remote certificate server.

## Syntax

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

## Parameters

*trustpointCA\_name*

Defines the name of the trust point you are enrolling. This name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

**directory** *remote\_dir\_name*

Defines the path of the directory to export the Certificate Signing Request.

**host** *host\_address*

Defines the host name or IP address of the remote certificate server.

**protocol** {FTP | SCP}

Specifies the use of either FTP or SCP protocol for exporting the certification file.

**user** *host\_login*

Defines user name for the host server.

**password** *host\_user\_password*

Defines the password for the user name on the host server.

### NOTE

It is recommended to not list the password in command line for security purposes; the user will be prompted for the password.

**country** *country*

Defines the two-letter country code for generating the CSR.

**state** *state*

Defines the state name for generating the CSR.

**locality** *locality*

Defines the locality name for generating the CSR.

**organization** *organization*

Defines the organizational unit name for generating the CSR.

**orgunit** *orgunit*

Defines the name of the certification file.

**common** *common\_name*

This is the name used to connect to the device through HTTPS. Enter a Fully Qualified Domain Name (FQDN) or IP address. If a FQDN is used, you need to configure a domain name and name server on the device.



## Modes

Privileged EXEC mode

## Usage Guidelines

The *trustpoint\_CAname* name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command.

## Examples

Typical command example:

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# crypto ca import

Imports the Identity Certificate for HTTPS security configuration.

## Syntax

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

```
no crypto ca import {trustpointCA_name}
```

## Parameters

*trustpointCA\_name*

Defines the name of the trust point you are authenticating. This name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

**certificate directory** *remote\_dir\_name*

Defines the directory where the certification file resides.

**file** *cert\_file*

Defines the name of the certification file.

**host** *host\_address*

Defines the host name or IP address of the remote certificate server.

**protocol** {FTP | SCP}

Specifies the use of either FTP or SCP protocol for accessing the certification file.

**user** *host\_login*

Defines user name for the host server.

**password** *host\_user\_password*

Defines the password for the user name on the host server.

### NOTE

It is recommended to not list the password in command line for security purposes; the user will be prompted for the password.

## Modes

Privileged EXEC mode

## Usage Guidelines

The *trustpoint\_CAname* name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command.

Use the no form of the command to remove the Identity Certificate.

## Examples

Typical command example:

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# crypto ca trustpoint

Defines the trust point for HTTPS security configuration.

## Syntax

`crypto ca trustpoint trustpointCA_name`

`no crypto ca trustpoint trustpointCA_name`

## Parameters

*trustpointCA\_name*

Defines the name of the trust point. The string for the name can not be left blank. The length of the string can range from 1 through 64 characters.

## Modes

Global configuration mode

## Usage Guidelines

Use the `no crypto ca trustpoint` command to remove the trust point.

## Examples

Typical command example:

```
device(config)# crypto ca trustpoint t1
```

Example using the no form of the command:

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# crypto key

Generates an RSA/ECDSA/DSA key pair to sign or encrypt and decrypt the security payload during security protocol exchanges for applications. You must sign and/or encrypt and decrypt the RSA/ECDSA/DSA key pair before you obtain a certificate for your device.

## Syntax

```
crypto key label key_label [rsa | ecdsa | dsa] [modulus key_size]
```

```
no crypto key label key_label
```

## Parameters

**label** *key\_label*

The name of the key pair.

**rsa**

Generates an RSA key pair.

**ecdsa**

Generates an ECDSA key pair.

**dsa**

Generates a DSA key pair.

**modulus** *key\_size*

Specifies the key size. The corresponding key sizes supported for each key type are:

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

## Modes

Global configuration mode

## Usage Guidelines

Use the no form of this command to remove the key pair.

The key label must contain alphanumeric characters.

## Examples

Typical command example for generating the key pair.

```
device(config)# crypto key label k1 rsa modulus 2048
device(config)# do show running-config crypto
crypto key label k1 rsa modulus 2048
```

The following is an example of using the no form of the command:

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# csnp-interval

Configures the Complete Sequence Number PDU (CSNP) interval.

## Syntax

```
csnp-interval secs
no csnp-interval
```

## Command Default

The default CSNP interval is 10 seconds.

## Parameters

`secs`  
Specifies the interval in seconds. Valid values range from 0 through 65535 seconds.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The interval configured on the device applies to both Level 1 and Level 2 CSNPs and Partial Sequence Number PDUs (PSNPs).

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

## Examples

The following example configures a CSNP interval of 25 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# csnp-interval 25
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# cspf-computation-mode

The path calculation metric implementation allows you to specify the path calculation for a given tunnel.

## Syntax

```
cspf-computation-mode { [ ignore-overload-bit | metric-type [ use-igp-metric | use-te-metric ] ] }
no cspf-computation-mode { [ ignore-overload-bit | metric-type [ use-igp-metric | use-te-metric ] ] }
```

## Command Default

By default, all LSPs use the global configuration.

## Parameters

### ignore-overload-bit

Ignores the overload bit during CSPF computation.

### metric-type

Select for CSPF computation.

### use-igp-metric

Use the IGP metric of the link for CSPF computation.

### use-te-metric

Use the TE metric of the link for CSPF computation.

## Modes

Global level (config-router-mpls-policy): This configuration covers all RSVP LSPs (primary, secondary LSPs).

Individual LSP mode: This configuration covers all RSVP LSPs.

## Usage Guidelines

The CLI configuration at the LSP level always overrides the configuration at the global level. That is, the decision to **use-te-metric** or **use-igp-metric** for CSPF path calculation if configured at the LSP level, always overrides the configuration at the global level/

The **no** form of the command removes the CSPF computation mode.

## Examples

In the following example, the CSPF computation mode is set back to a default value of the te-metric at the global level.

```
device# configure
device(config)# router-mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)#cspf-computation-mode metric-type use-igp-metric
device(config-router-mpls-policy)#no cspf-computation-mode metric-type use-te-metric
Error:CSPF computation is configured to use igp-metric
device(config-router-mpls-policy)#no cspf-computation-mode metric-type use-igp-metric
```



In the following example, the CSPF computation mode is set back to a default value of the use-te-metric at the LSP level.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp test
device(config-router-mpls-lsp-test)# cspf-computation-mode metric-type use-igp-metric
device(config-router-mpls-policy)#no cspf-computation-mode metric-type use-te-metric
Error:CSPF computation is configured to use-igp-metric
device(config-router-mpls-policy)#no cspf-computation-mode metric-type use-igp-metric
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# cspf-interface-constraint

Forces the CSPF calculation to include any specified interface when creating an LSP.

## Syntax

`cspf-interface-constraint`

`no cspf-interface-constraint`

## Command Default

The command is disabled, by default.

## Modes

MPLS policy mode.

## Usage Guidelines

The command may be dynamically turned on or off. Turning the command off or on has no effect on LSPs that have already been established (primary and secondary). For LSPs that are currently retried, changing the constraint setting changes the behavior on the next retry such as when an LSP whose path is configured to use that interface fails to come up due to an interface down condition.

The command has significance for the ingress node only, where the CSPF calculation takes place for an LSP or a detour segment.

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

## Examples

The following example configures the command.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-interface-constraint
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# cspf-group

Configures a CSPF fate-sharing group by assigning a name to the group.

## Syntax

```
cspf-group { group_name }
no cspf-group
```

## Command Default

The command is disabled by default.

## Parameters

*group\_name*

Specifies the name of the fate-sharing group. The group-name variable can be up to 128 characters. The objects that can be specified for a fate-sharing group are interface, point-to-point link, node, and subnet.

## Modes

MPLS router mode.

## Usage Guidelines

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

## Examples

The following example assigns the name *group3* to the fate sharing group configuration.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# cspf-group group3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# cspf-group-computation

Specifies the mode that is used when setting up a fate-sharing group.

## Syntax

```
cspf-group-computation [ add-penalty ]
no cspf-group-computation
```

## Command Default

The CSPF group computation mode is disabled, by default.

## Parameters

### add-penalty

Specifies the penalty that is added from all CSPF groups associated with the same TE link used by the protected path.

## Modes

MPLS policy mode (config-router-mpls-policy).

## Usage Guidelines

the no form of the command disables the CSPF group computation mode.

## Examples

The following example specifies the CSPF-group computation for a fate sharing group, and enables the add-penalty option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-group-computation add-penalty
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dampening

Sets dampening parameters for the route in BGP address-family mode.

## Syntax

```
dampening { half-life reuse suppress max-suppress-time | route-map route-map }
no dampening
```

## Command Default

Disabled.

## Parameters

*half-life*

Number of minutes after which the route penalty becomes half its value. Range is from 1 through 45. Default is 15.

*reuse*

Minimum penalty below which the route becomes usable again. Range is from 1 through 20000. Default is 750.

*suppress*

Maximum penalty above which the route is suppressed by the device. Range is from 1 through 20000. Default is 2000.

*max-suppress-time*

Maximum number of minutes a route can be suppressed by the device. Range is from 1 through 255. Default is 40.

*route-map*

Enables selection of dampening values established in a route map by means of the **route-map** command.

*route-map*

Name of the configured route map.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

## Usage Guidelines

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

Use **dampening** without operands to set default values for all dampening parameters.

To use the dampening values established in a route map, configure the route map first, and then enter the **route-map** command, followed by the name of the configured route map.

A full range of dampening values (*half-life, reuse, suppress, max-suppress-time*) can also be set by means of the **set as-path prepend** command.

## Examples

The following example enables default dampening as an IPv4 address-family function.

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

The following example changes all the dampening values as an IPv6 address-family function.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# dampening 20 200 2500 40
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# database-overflow-interval (OSPFv2)

Configures frequency for monitoring database overflow.

## Syntax

```
database-overflow-interval interval  
no database-overflow-interval
```

## Command Default

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

## Parameters

*interval*

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds.

## Modes

OSPF router configuration mode  
OSPF router VRF configuration mode

## Usage Guidelines

This command specifies how long a device that has entered the OverflowState waits before resuming normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the device lapses back into OverflowState. If the configured value of the database overflow interval is zero, then the device never leaves the database overflow condition.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the device enters OverflowState. In this state, the device flushes all non-default AS-external-LSAs that the device had originated. The device also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

The **no** form of the command disables the overflow interval configuration.

## Examples

The following example configures a database-overflow interval of 60 seconds.

```
device# configure terminal  
device(config)# router ospf  
device(config-router-ospf-vrf-default-vrf)# database-overflow-interval 60
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# database-overflow-interval (OSPFv3)

Configures frequency for monitoring database overflow.

## Syntax

```
database-overflow-interval interval  
no database-overflow-interval
```

## Command Default

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

## Parameters

*interval*

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds (24 hours).

## Modes

OSPFv3 router configuration mode  
OSPFv3 router VRF configuration mode

## Usage Guidelines

This command specifies how long after a router that has entered the OverflowState before it can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

The **no** form of the command disables the overflow interval configuration.

## Examples

The following example configures a database-overflow interval of 120 seconds.

```
device# configure terminal  
device(config)# ipv6 router ospf  
device(config-ipv6-router-ospf-vrf-default-vrf)# database-overflow-interval 120
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug access-list-log buffer

Configures or clears the ACL buffer.

## Syntax

Configure the ACL buffer:

```
debug access-list-log buffer { circular | linear } packet-count count_value
```

Clear the ACL buffer:

```
debug access-list-log buffer clear
```

Disable the ACL buffer:

```
no debug access-list-log buffer
```

## Parameters

**circular** | **linear**

Specifies the buffer type.

**packet-count** *count\_value*

Specifies a value from 64 through 2056.

**clear**

Clears the buffer contents.

## Modes

Privileged EXEC mode

## Usage Guidelines

D diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug dhcp packet buffer

Configures a buffer to capture DHCP packets.

## Syntax

```
debug dhcp packet buffer [all | circular packet count | clear vrf name | interface ethernet/port-channel | linearpacket count]
```

## Command Default

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

## Parameters

### circular

Buffer wraps around to overwrite earlier captures.

### linear

Buffer stops capture when the packet-count value is reached.

### clear

Clears the packet buffer.

### all

Captures DHCP packets on all interfaces.

### interface

Represents a valid interface such as Ethernet or port channel.

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

This command configures the capturing buffer behavior by allowing captures to wrap and overwrite earlier captures or stop capturing when a packet-count limit is reached. The current buffer content is cleared when the configuration changes.

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

## Examples

The following example configures a buffer to capture 510 maximum packets in a circular fashion.

```
device# debug dhcp packet buffer circular packet-count 510
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug ip bgp

Displays information related to the processing of BGP4, with a variety of options.

## Syntax

```
debug ip bgp { cli | dampening | events | general | graceful-restart | ip-prefix ip-addr/mask-len | ip-prefix-list name |
  keepalives | route-map name | route-selection | traces | updates [ rx | tx ] } [ all-vrfs | vrf vrf-name ]
```

```
no debug ip bgp
```

## Parameters

### cli

Displays information about BGP CLI

### dampening

Displays BGP4 dampening.

### events

Displays all BGP4 events.

### general

Displays BGP4 common events.

### graceful-restart

Displays BGP graceful restart events.

### ip-prefix

Displays information filtered by IP prefix.

*ip-addr*

IPv4 address in dotted-decimal notation.

*mask-len*

IPv4 mask length in CIDR notation.

### ip-prefix-list

Displays information filtered by IP prefix list.

*name*

Name of IP prefix list.

### keepalives

Displays BGP4 keepalives.

### route-map

Displays configured route map tags.

*name*

Name of route map.

### route-selection

Displays BGP4 route selection.

### traces

Displays BGP traces.

**updates**

Displays BGP4 updates.

**rx**

Displays BGP4 received updates.

**tx**

Displays BGP4 transmitted updates

**all-vrfs**

Specifies all VRFs.

**vrf**

Specifies a VRF instance or all VRFs.

*vrf-name*

Specifies a VRF instance

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

If you want to see BGP4 keepalives for a specific neighbor, you must first specify the neighbor using the **debug ip bgp neighbor** command. Only keepalive traces for the specified neighbor will appear in the debugging message.

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

## Examples

The following example sets debugging on BGP4 events.

```
device# debug ip bgp events
```

The following example sets debugging on BGP4 graceful restart events.

```
device# debug ip bgp graceful-restart
```

The following example specifies that BGP4 keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive
device# debug ip bgp neighbor 10.1.1.1
```

The following example sets debugging on BGP4 events for VRF instance "red".

```
device# debug ip bgp events vrf red
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug ip bgp neighbor

Displays information related to the processing of BGP4 for a specific neighbor.

## Syntax

```
debug ip bgp neighbor ip-addr [ all-vrfs | vrf vrf-name ]  
no debug ip bgp neighbor ip-addr [ all-vrfs | vrf vrf-name ]
```

## Parameters

*ip-addr*  
IPv4 address in dotted-decimal notation.

**all-vrfs**  
Specifies all VRFs.

**vrf**  
Specifies a VRF instance or all VRFs.

*vrf-name*  
Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

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

## Examples

The following example sets debugging on information related to the processing of BGP4 for a specific neighbor.

```
device# debug ip bgp neighbor 10.11.12.13
```

The following example specifies that BGP4 keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive  
device# debug ip bgp neighbor 10.1.1.1
```

The following example sets debugging on information related to the processing of BGP4 for a specific neighbor for VRF instance "red".

```
device# debug ip bgp neighbor 10.11.12.13 vrf red
```

The following example sets debugging information related to the processing of BGP4 for a specific neighbor for all VRFs.

```
device# debug ip bgp neighbor 10.11.12.13 all-vrfs
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# debug ip igmp

Enables or disables debugging for IGMP information.

## Syntax

```
debug ip igmp { all | errors | group A.B.C.D | packet | rx | tx | interface ethernet | port-channel tunnel | vlan vlan_id }  
no debug ip igmp
```

## Parameters

### all

Enables all debugs.

### errors

Enables only error type debugs, such as memory allocation failures etc.

### group A.B.C.D

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

### packet

Enables debug for query/reports per the chosen option.

### rx

Specifies only ingressing flow debugs to be captured in traces.

### tx

Specifies only egressing packet flows to be captured in traces.

### interface

Specifies the interface (ethernet, port-channel, tunnel) to be monitored.

### vlan

Specifies the VLAN to be monitored.

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

When debugging is enabled, all of the IGMP packets received and sent and IGMP-host related events are displayed.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug ip pim

Enables debugging for IP Protocol Independent Multicast.

## Syntax

```
debug ip pim { add-del-oif | bootstrap | group | join-prune | nbr-change | packets | parent | regproc | route-change | rp |  
source | state | all }
```

```
no debug ip pim all
```

## Command Default

All flags are disabled.

## Parameters

### add-del-oif

Controls the OIF change flag.

### bootstrap

Controls the bootstrap processing flag.

### group

Controls the processing for a group flag.

### join-prune

Controls the Join/Prune processing flag.

### nbr-change

Controls the neighbor changes flag.

### packets

Controls the packet processing flag.

### parent

Controls the parent change processing flag.

### regproc

Controls the register processing flag.

### route-change

Controls the route changes flag.

### rp

Controls the Rendezvous Point (RP) processing flag.

### source

Controls the processing for a source flag.

### state

Controls the state processing flag.

### all

Controls all of the states.

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

Use the **no debug ip pim all** command to disable debugging.

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug ipv6 bgp

Displays debug information related to BGP processing for IPv6 prefix lists.

## Syntax

```
debug ipv6 bgp ipv6-prefix ipv6-address /mask [ all-vrfs | vrf vrf-name ]
debug ipv6 bgp ipv6-prefix name [ all-vrfs | vrf vrf-name ]
debug ipv6 bgp ipv6-prefix-list name [ all-vrfs | vrf vrf-name ]
no debug ipv6 bgp ipv6-prefix ipv6-address /mask [ all-vrfs | vrf vrf-name ]
no debug ipv6 bgp ipv6-prefix name [ all-vrfs | vrf vrf-name ]
no debug ipv6 bgp ipv6-prefix-list name [ all-vrfs | vrf vrf-name ]
```

## Parameters

*ipv6-address /mask*

Specifies an IPv6 address and network mask.

**all-vrfs**

Specifies all VRFs.

**vrf**

Specifies a VRF instance or all VRFs.

*vrf-name*

Specifies a VRF instance

*name*

Specifies a prefix list name.

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

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

## Examples

This example enables debugging for IPv6 prefix list "myv6list" for VRF instance "red".

```
device# debug ipv6 bgp ipv6-prefix-list myv6list vrf red
```

This example enables debugging for a specified IPv6 address for all VRFs.

```
device# debug ipv6 bgp ipv6-prefix 2001::/16 all-vrfs
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug ipv6 bgp neighbor

Displays debug information related to BGP processing for a specified neighbor.

## Syntax

```
debug ipv6 bgp neighbor ipv6-addr [ all-vrfs | vrf vrf-name ]  
no debug ipv6 bgp neighbor ipv6-addr [ all-vrfs | vrf vrf-name ]
```

## Command Default

None

## Parameters

*ipv6-addr*

IPv6 address of a neighbor.

**all-vrfs**

Specifies all VRFs.

**vrf**

Specifies a VRF instance or all VRFs.

*vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

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

## Examples

The following example sets debugging for a neighbor.

```
device# debug ipv6 bgp neighbor 2000::1
```

The following example specifies that BGP keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive  
device# debug ipv6 bgp neighbor 2001::1
```

The following example sets debugging for a neighbor for VRF instance "red".

```
device# debug ipv6 bgp neighbor 2000::1 vrf red
```



The following example sets debugging for a neighbor for all VRFs.

```
device# debug ipv6 bgp neighbor 2000::1 all-vrfs
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# debug udd packet

Enables debugging for the Unidirectional Link Detection (UDLD) protocol.

## Syntax

```
debug udd packet [ all | { interface [ ethernet slot/port ] } { both | rx | tx }  
no debug udd packet
```

## Command Default

UDLD debugging is disabled.

## Parameters

- all**  
Activates UDLD debugging on all ports on the switch.
- ethernet**  
Represents a valid, physical Ethernet type for all available Ethernet speeds.
- slot/port*  
Specifies a valid slot and port number.
- both**  
Sets debugging for both received and transmitted packets.
- rx**  
Sets debugging for received packets only.
- tx**  
Sets debugging for transmitted packets only.

## Modes

Privileged EXEC mode

## Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Please work closely with Extreme Networks technical support in running **debug** or **show system internal** commands and interpreting their results.

When debugging is enabled UDLD PDUs are written to the console as they are transmitted and/or received on one or all ports.

Use the **show debug udd** command to view your current debug settings.

Use the **no** form of this command to turn off either all dumping of UDLD PDUs or dumping on a specific port.

## Examples

To turn on debugging of transmitted packets on a specific ethernet interface:

```
device# debug uuld packet interface ethernet 5/1 tx
```

## History

Release version	Command history
7.0.0	This command was modified to include updated Usage Guidelines.

# default-information-originate (BGP)

Configures the device to originate and advertise a default BGP route.

## Syntax

**default-information-originate**

**no default-information-originate**

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

The following example originates and advertises a default BGP4 route.

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

The following example originates and advertises a default BGP4+ route for VRF "red".

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-information-originate (IS-IS)

Generates a default route into an Intermediate System-to-Intermediate System (IS-IS) routing domain.

## Syntax

```
default-information-originate [ route-map name ]
```

```
no default-information-originate [ route-map name ]
```

## Command Default

Disabled.

## Parameters

**route-map** *name*

Specifies that the default route is generated if the route map is satisfied. The route map name can be from 1 through 63 characters in length.

## Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

## Usage Guidelines

The **no** form of the command disables default route origination.

## Examples

The following example generates a default external route into an IS-IS domain.

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

The following example generates a default external route into an IS-IS domain if the route map "myroutemap" is satisfied

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# default-information-originate route-map myroutemap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-information-originate (OSPFv2)

Controls distribution of default information to an OSPFv2 device.

## Syntax

```
default-information-originate [ always ] [ metric metric ] [ metric-type { type1 | type2 } ] [ route-map name ]
no default-information-originate
```

## Command Default

The default route is not advertised into the OSPFv2 domain.

## Parameters

### always

Always advertises the default route. If the route table manager does not have a default route, the router advertises the route as pointing to itself.

### metric *metric*

specifies the cost for reaching the rest of the world through this route. If you omit this parameter and do not specify a value using the *default-metric* router configuration command, a default metric value of 1 is used. Valid values range from 1 through 65535. The default is 10.

### metric-type

Specifies how the cost of a neighbor metric is determined. The default is **type1**. However, this default can be changed with the **metric-type** command.

#### type1

Type 1 external route.

#### type2

Type 2 external route.

### route-map *name*

Specifies that the default route is generated if the route map is satisfied. This parameter overrides other options. If the **set metric** and **set metric-type** commands are specified in the route-map, the command-line values of metric and metric-type if specified, are "ignored" for clarification.

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the route table manager (RTM), whether static or learned from another protocol, to its neighbors.

The corresponding route-map should be created before configuring the **route-map** option, along with the **default-information-originate** command. If the corresponding route-map is not created beforehand, an error message is displayed stating that the route-map must be created.

The route-map option cannot be used with a non-default address in the match conditions. The default route LSA is not generated if a default route is not present in the routing table and a **match ip address** condition for an existing non-default route is configured in the route-map. The **match ip address** command in the route-map is a no-op operation for the default information originate command.

The **no** form of the command disables default route origination.

## Examples

The following example creates and advertises a default route with a metric of 30 and a type 1 external route.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-information-originate metric 30 metric-type type1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-information-originate (OSPFv3)

Controls distribution of default information to an OSPFv3 device.

## Syntax

```
default-information-originate [ always ] [ metric metric ] [ metric-type { type1 | type2 } ]
no default-information-originate
```

## Command Default

The default route is not advertised into the OSPFv3 domain.

## Parameters

### always

Always advertises the default route. If the route table manager (RTM) does not have a default route, the router advertises the route as pointing to itself.

### metric *metric*

Used for generating the default route, this parameter specifies the cost for reaching the rest of the world through this route. If you omit this parameter, the value of the **default-metric** command is used for the route. Valid values range from 1 through 65535.

### metric-type

Specifies the external link type associated with the default route advertised into the OSPF routing domain.

#### type1

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

The default is **type1**.

#### type2

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

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the RTM (whether static or learned from another protocol) to its neighbors.

The **no** form of the command disables default route origination.



## Examples

The following example specifies a metric of 20 for the default route redistributed into the OSPFv3 routing domain and an external metric type of Type 2.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# default-information-originate metric 20 metric-type
type2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-link-metric

Configures the metric value globally on all active Intermediate System-to-Intermediate System (IS-IS) interfaces for a specified address family.

## Syntax

```
default-link-metric { level-1 | level-2 } value
```

```
no default-link-metric { level-1 | level-2 }
```

## Command Default

Disabled.

## Parameters

### level-1

Specifies the default-link-metric parameter as Level 1.

### level-2

Specifies the default-link-metric parameter as Level 2.

### value

Specifies the default-link-metric value in metric style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default is 10.

## Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

## Usage Guidelines

This command is useful when you have a common IS-IS metric value on all IS-IS interfaces (other than the default metric value of 10). This command is not applicable to MPLS IS-IS shortcuts and tunnel interfaces.

If you change the metric style configuration, the value of the default link metric also changes. The new value of the default link metric is equal to the minimum of the configured value and the maximum value supported by the new metric style. For example, if the metric style changes from wide metric to narrow metric, and the default-link-metric value is greater than 63, the default-link-metric value changes to 63 because it is the maximum value supported in the narrow metric style. When the metric style changes from a narrow metric to a wide metric, there is no change to the default-link-metric value.

You can change the metric value for a specific interface using the **isis metric** command or the **isis ipv6 metric** command. The **isis metric** command configuration takes precedence over the **default-link metric value** command configuration.

The **no** form of the command resets the metric value to the default value 10.

## Examples

The following example configures the IS-IS default-link-metric value to 30 for Level 1 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-link-metric level-1 30
```

The following example configures the IS-IS default-link-metric value to 30 for Level 1, and the IS-IS default-link-metric value to 40 for Level 2 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family-ipv6 unicast
device(config-router-isis-ipv6u)# default-link-metric level-1 30
device(config-router-isis-ipv6u)# default-link-metric level-2 40
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-local-preference

Enables setting of a local preference value to indicate a degree of preference for a route relative to that of other routes.

## Syntax

```
default-local-preference num
no default-local-preference
```

## Command Default

The default local preference is 100.

## Parameters

*num*  
Local preference value. Range is from 0 through 65535.

## Modes

BGP configuration mode

## Usage Guidelines

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

Use this command to change the local preference value. Local preference indicates a degree of preference for a route relative to that of other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message.

## Examples

This example sets the local preference value to 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# default-local-preference 200
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-metric (BGP)

Changes the default metric used for redistribution.

## Syntax

**default-metric** *value*

**no default-metric**

## Command Default

The default metric value is 1.

## Parameters

*value*

Metric value. Range is from 0 through 4294967295.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

The following example changes the default metric used for redistribution to 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# default-metric 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-metric (IS-IS)

Sets the default redistribution metric value for the Intermediate System-to-Intermediate System (IS-IS) routing protocol.

## Syntax

**default-metric** *value*

**no default-metric**

## Command Default

The default metric value is 0.

## Parameters

*value*

Specifies the default metric value. Valid values range from 0 through 65535. The default is 0.

## Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

## Usage Guidelines

The **no** form of the command resets the default metric value to the default value of 0.

## Examples

The following example sets the default metric value to 20 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-metric 20
```

The following example sets the default metric value to 40 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# default-metric 40
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-metric (OSPF)

Sets the default metric value for the OSPFv2 or OSPFv3 routing protocol.

## Syntax

```
default-metric metric
no default-metric
```

## 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-router-ospf-vrf-default-vrf)# default-metric 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# default-passive-interface

Marks all OSPFv2 and OSPFv3 interfaces passive by default.

## Syntax

**default-passive-interface**

**no default-passive-interface**

## Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

When you configure the interfaces as passive, the interfaces drop all the OSPFv2 and OSPFv3 control packets.

You can use the **ip ospf active** and **ip ospf passive** commands in interface subconfiguration mode to change active/passive state on specific OSPFv2 interfaces. You can use the **ipv6 ospf active** and **ipv6 ospf passive** commands in interface subconfiguration mode to change the active and passive state on specific OSPFv3 interfaces.

The **no** form of the command disables the passive state.

## Examples

The following example marks all OSPFv2 interfaces as passive.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-passive-interface
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# delay

For an implementation of an event-handler profile, specifies a delay from when a trigger is received until execution of the event-handler action.

## Syntax

**delay** *seconds*

**no delay**

## Command Default

There is no delay from when a trigger is received until execution of the event-handler action.

## Parameters

*seconds*

Specifies the number of seconds from when a trigger is received until the execution of the specified action begins. Valid values are 0 or a positive integer.

## Modes

Event-handler activation mode

## Usage Guidelines

The **no** form of this command resets the **delay** setting to the default 0 seconds.

## Examples

The following example specifies a delay of 60 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# delay 60
```

The following example resets **delay** to the default value of 0 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no delay
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# delay-link-event

Configures the port transition hold timer to set a delay in the sending of port up or down port events, or both, to Layer 2 protocols.

## Syntax

**delay-link-event** *multiple-iteration* { **down** | **up** | **both** }

**no delay-link-event**

## Command Default

The sending of an up or down port event is not delayed.

## Parameters

*multiple-iteration*

Specifies the number of times that the polling iteration occurs. Enter an integer from 1 to 200. The polling iteration is 50 ms. The delay time is the *multiple-iteration* times 50 ms.

**both**

Sets the delay for the port down and up events.

**down**

Sets the delay for the port down event.

**up**

Sets the delay for the port up event.

## Modes

Interface Ethernet configuration mode.

## Usage Guidelines

Use the **no** form of the command to remove the delay from the port events on the interface.

While link down events are reported immediately in the Syslog, their effect on higher level protocols such as OSPF is delayed according to how the hold timer is configured. When configured, the timer affects the physical link events. However, the resulting logical link events are also delayed.

### NOTE

All LAG member ports must have the same delayed-link-event configuration.

### NOTE

The delayed-link-event configuration is applicable only on a physical interface. It is not valid on a VLAN, VE, LAG, or loopback interfaces.

**NOTE**

The port transition hold timer does not take effect when the interface is administratively shut down.

## Examples

The following example shows the steps in the previous configuration.

```
device# configure terminal
device(config)# interface Ethernet 4/2
device(conf-if-eth-4/2)# delay-link-event 2 down
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# delete

Deletes a user-generated file from the flash memory.

## Syntax

**delete** *file*

## Parameters

*file*

The name of the file to be deleted.

## Modes

Privileged EXEC mode

## Usage Guidelines

The delete operation is final; there is no mechanism to restore the file.

System configuration files cannot be deleted. If you try to delete a system configuration file, an appropriate message is displayed.

## Examples

To delete a user-generated copy of a configuration file:

```
device# delete myconfig

% Warning: File will be deleted (from flash:)!
Continue?(y/n): y
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# deploy

Deploys the MCT cluster or cluster client to bring the MCT device to operational mode .

## Syntax

**deploy**  
**no deploy**

## Modes

Cluster and cluster client configuration mode

## Usage Guidelines

Before deploying a cluster, the cluster client must be configured.

Before deploying a cluster client, the client interface and ESI settings must be configured under the client configuration.

An LSP is automatically created when you deploy a cluster. When you undeploy a cluster, the LSP is removed.

The client will not operate in MCT mode unless the remote client is also deployed.

The **no** form of the command undeploys the cluster or the client cluster.

When the client is undeployed, all MAC addresses are removed locally and a withdraw message is sent to the MCT peer to remove all associated client MAC addresses.

## Examples

The following example shows the deployment of a cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# deploy
```

The following example shows the deployment of a cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# deploy
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# designated-forwarder-hold-time

Configures the time in seconds to wait before electing a designated forwarder.

## Syntax

`designated-forwarder-hold-time seconds`

`designated-forwarder-hold-time`

## Command Default

The default setting is three seconds.

## Parameters

*seconds*

Specifies the hold time in seconds. Enter an integer from 1 to 60.

## Modes

Cluster configuration mode

## Usage Guidelines

Use the **no** form of the command to reset the default setting of three seconds.

The designated forwarder is a PE in a set of multi-homing PEs connected to the same Ethernet segment that is responsible for sending BUM traffic to a client for a particular VLAN ID on an Ethernet segment.

DF election is not triggered unless at least one remote CCEP is configured. When a CCEP goes up or down, DF election is triggered as soon as the Ethernet route acknowledgment from remote peer is received.

When a client is deployed locally or remotely, or the BGP session comes up, the DF timer does not start and DF election is not performed until the timer expired.

## Examples

The following example configures a 20-second hold time for DF election.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# designated-forwarder-hold-time 20
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# description

Defines a description for an event-handler profile.

## Syntax

**description** *description-text*

**no description**

## Command Default

No description is defined.

## Parameters

*description-text*

Characters describing the event-handler profile. The string can be 1 through 128 ASCII characters in length. Do not use the ? character. If you need to use ! or \, precede each with \.

## Modes

Event-handler configuration mode

## Usage Guidelines

An event-handler profile supports only one description.

To delete a description, use the **no** form of this command.

To change a description, you do not need to first delete the existing description. Just create a new description.

## Examples

The following example defines a description for eventHandler1.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)# description This is a sample description.
```

## History

Release version	Command history
7.0.0	This command was introduced.

# description (LLDP)

Specifies a string that contains the LLDP description.

## Syntax

**description** *string*

**no description**

## Parameters

*string*

Characters describing LLDP. The string must be between 1 and 50 ASCII characters in length.

## Modes

Protocol LLDP and profile configuration modes

## Usage Guidelines

Enter **no description** to remove the LLDP description.

The LLDP description can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

## Examples

To set the strings describing LLDP:

```
device(conf-lldp)# description Extreme-LLDP
```

To set the strings describing LLDP for a specific LLDP profile, test2, enter the following:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# description test2
device(config-profile-test1)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# description (STP)

Describes an xSTP configuration.

## Syntax

**description** *description*

**no description**

## Parameters

*description*

Characters describing the xSTP configuration. The string must be between 1 and 64 ASCII characters in length.

## Modes

xSTP configuration mode

## Usage Guidelines

Enter **no description** to remove the description.

## Examples

To specify the bridge priority:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# description STP-S1
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# description RSTP-S1
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# description MSTP-S1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# description (VRRP)

Describes a Virtual Router Redundancy Protocol extended (VRRP-E) interface.

## Syntax

**description** *description*

**no description**

## Parameters

*description*

Characters describing the VRRP-E interface. The string must be between 1 and 64 ASCII characters in length.

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

Enter **no description** to remove the description.

## Examples

To describe the VRRP-E group 10 interface:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# description vrrpe_group_10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# destination

Configures the destination address for the tunnel interface.

## Syntax

**destination** *ip-address*

**no destination** *ip-address*

## Command Default

No tunnel interface destination is configured.

## Parameters

*ip-address*

Specifies the IPv4 address.

## Modes

Interface tunnel configuration mode

## Usage Guidelines

Use the **no tunnel destination** command to remove the destination configuration.

You must ensure that a route to the tunnel destination exists on the tunnel source device and create a static route if necessary.

## Examples

This example configures the IP address 10.1.2.3 as the destination address.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# destination 10.1.2.3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## dir

Lists the contents of the device flash memory.

## Syntax

dir

## Modes

Privileged EXEC mode

## Examples

The following example lists the contents of the flash memory.

```
device# dir
total 572
drwxr-xr-x 2 251 1011 4096 Jun 5 07:08 .
drwxr-xr-x 3 251 1011 4096 Mar 11 00:00 ..
-rw-r--r-- 1 root sys 410 Jun 3 00:56 defaultconfig.standalone
-rw-r--r-- 1 root sys 695 Jun 3 00:56 defaultconfig.cluster
-rw-r--r-- 1 root root 185650 Jun 5 09:38 startup-config
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# disable-adjacency-check

Disables Intermediate System-to-Intermediate System (IS-IS) IPv6 protocol-support consistency checks that are performed prior to forming adjacencies on hello packets.

## Syntax

```
disable-adjacency-check
no disable-adjacency-check
```

## Command Default

Disabled.

## Modes

IS-IS address-family IPv6 unicast configuration mode

## Usage Guidelines

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

## Examples

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

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

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

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# disable-incremental-spf-opt

Disables incremental full SPF optimizations for Intermediate System-to-Intermediate System (IS-IS).

## Syntax

```
disable-incremental-spf-opt
```

```
no disable-incremental-spf-opt
```

## Command Default

Disabled.

## Modes

IS-IS router configuration mode

## Usage Guidelines

If you disable the partial SPF optimizations using the **disable-partial-spf-opt** command, IS-IS automatically disables the incremental SPF optimizations and always runs full SPF. However, if you disable incremental SPF optimizations using this command, IS-IS does not disable partial optimizations.

The **no** form of the command restores incremental SPF optimizations for IS-IS.

## Examples

The following example disables incremental SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-incremental-spf-opt
```

The following example restores incremental SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no disable-incremental-spf-opt
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# disable-inc-stct-spf-opt

Disables incremental shortcut LSP SPF optimization.

## Syntax

```
disable-inc-stct-spf-opt
```

```
disable-inc-stct-spf-opt
```

## Command Default

Disabled.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command restores incremental shortcut LSP SPF optimization.

## Examples

The following example disables incremental shortcut LSP SPF optimization.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-inc-stct-spf-opt
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# disable-partial-spf-opt

Disables partial SPF optimizations for Intermediate System-to-Intermediate System (IS-IS).

## Syntax

```
disable-partial-spf-opt
no disable-partial-spf-opt
```

## Command Default

Disabled.

## Modes

IS-IS router configuration mode

## Usage Guidelines

If you disable the partial SPF optimizations using this command, IS-IS automatically disables the incremental SPF optimizations and always runs full SPF. However, if you disable incremental SPF optimizations using the **disable-incremental-spf-opt** command, IS-IS does not disable partial optimizations.

The **no** form of the command restores partial SPF optimizations for IS-IS.

## Examples

The following example disables partial SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-partial-spf-opt
```

The following example restores partial SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no disable-partial-spf-opt
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# distance (BGP)

Changes the default administrative distances for eBGP, iBGP, and local BGP.

## Syntax

**distance** *external-distance internal-distance local-distance*

**no distance**

## 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-router)# distance 100 150 200
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## distance (IS-IS)

Configures an administrative distance value for Intermediate System-to-Intermediate System (IS-IS) routes.

### Syntax

**distance** *number*

**no distance** *number*

### Command Default

The default is 115.

### Parameters

*value*

Specifies the administrative distance. Valid values range from 1 through 255. The default is 115.

### Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

### Usage Guidelines

Routes with a distance value of 255 are not installed in the routing table.

The **no** form of the command resets the distance value to the default value of 115.

### Examples

The following example sets an administrative distance of 40 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# distance 40
```

The following example sets an administrative distance of 60 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# distance 60
```

### History

Release version	Command history
16r.1.00	This command was introduced.

# distance (OSPF)

Configures an administrative distance value for OSPFv2 and OSPFv3 routes.

## Syntax

```
distance { external | inter-area | intra-area } distance  
no distance
```

## Command Default

The administrative distance value for OSPFv2 and OSPFv3 routes is 110.

## Parameters

### external

Sets the distance for routes learned by redistribution from other routing domains.

### inter-area

Sets the distance for all routes from one area to another area.

### intra-area

Sets the distance for all routes within an area.

### distance

Administrative distance value assigned to OSPF routes. Valid values range from 1 through 255. The default is 110.

## Modes

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

## Usage Guidelines

You can configure a unique administrative distance for each type of OSPF route.

The distances you specify influence the choice of routes when the device has multiple routes from different protocols for the same network. The device prefers the route with the lower administrative distance. However, an OSPFv2 or OSPFv3 intra-area route is always preferred over an OSPFv2 or OSPFv3 inter-area route, even if the intra-area route's distance is greater than the inter-area route's distance.

The **no** form of the commands reverts to the default setting.

## Examples

The following example sets the distance value for all external routes to 125.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distance external 125
```

The following example sets the distance value for intra-area routes to 80.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distance intra-area 80
```

The following example sets the distance value for inter-area routes to 90.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# distance inter-area 90
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# distribute-list prefix-list (OSPFv3)

Applies a prefix list to OSPF for IPv6 routing updates. Only routes permitted by the prefix-list can go into the routing table.

## Syntax

```
distribute-list prefix-list list-name in
no distribute-list prefix-list
```

## Command Default

Prefix lists are not applied to OSPFv3 for IPv6 routing updates.

## Parameters

*list-name*

Name of a prefix-list. The list defines which OSPFv3 networks are to be accepted in incoming routing updates.

**in**

Applies the prefix list to incoming routing updates on the specified interface.

## Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

## Usage Guidelines

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

## Examples

The following example configures a distribution list that applies the filterOspfRoutes prefix list globally:

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# distribute-list prefix-list filterOspfRoutes in
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# distribute-list route-map

Creates a route-map distribution list.

## Syntax

```
distribute-list route-map map in
no distribute-list route-map
```

## Parameters

*map*  
Specifies a route map.

**in**  
Creates a distribution list for an inbound route map.

## Modes

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

## Usage Guidelines

The distribution list can filter Link State Advertisements (LSAs) received from other OSPF devices before adding the corresponding routes to the routing table.

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

## Examples

The following example creates a distribution list using a route map named filter1 that has already been configured.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distribute-list route-map filter1 in
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x authentication

Enables 802.1x authentication on a port.

## Syntax

```
dot1x authentication
no dot1x authentication
```

## Command Default

802.1x authentication is disabled for ports.

## Modes

Interface configuration mode

## Usage Guidelines

Port control must be configured to activate authentication on an 802.1x-enabled interface using the **dot1x port-control auto** command from interface configuration mode.

Before activating the authentication using the **dot1x port-control auto** command on a port, you must remove configured static ACLs and static VLANs, if any, from the port.

Enter the **no dot1x authentication** command to disable dot1x on the port and remove the configuration from 802.1x management.

## Examples

The following example enables 802.1x authentication on a specific port:

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x authentication
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x enable

Enables 802.1X authentication globally.

## Syntax

```
dot1x enable
```

## Command Default

802.1x authentication is not enabled.

## Modes

Global configuration mode

## Usage Guidelines

The **dot1x enable** command enables 802.1x authentication globally on all ports.

### NOTE

802.1x port authentication is not supported by LAG (Link Aggregation Group) or interfaces that participate in a LAG.

## Examples

The following example enables 802.1X authentication globally on all interfaces.

```
device(config)# dot1x enable
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# dot1x filter-strict-security

Enables or disables strict filter security for dot1x authentication on the interface.

## Syntax

**dot1x filter-strict-security**

**no dot1x filter-strict-security**

## Command Default

Strict filter security is enabled.

## Modes

Interface configuration mode

## Usage Guidelines

By default, strict security mode is enabled; that is the client is not authenticated if the Filter-Id attribute returned by RADIUS contains invalid information, or if insufficient system resources are available to implement the IP ACLs or MAC address filters.

When strict security mode is enabled:

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

When strict security mode is disabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, a MAC address filter or IP ACL configured on the device), then the client is still authenticated, but no filter is dynamically applied to it.
- If the Vendor-Specific attribute specifies the syntax for a filter, but there are insufficient system resources to implement the filter, then the client is still authenticated, but the filter specified in the Vendor-Specific attribute is not applied to the port.

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

## Examples

The following example enables strict filter security.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x filter-strict-security
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## dot1x max-req

Configures the retransmission parameter that defines the maximum number of times EAP request/challenge frames are retransmitted when EAP response/identity frame is not received from the client.

### Syntax

```
dot1x max-req count
```

```
no dot1x max-req count
```

### Command Default

The device retransmits the EAP-request/challenge twice.

### Parameters

*count*

Specifies the number of EAP frame re-transmissions. Th range is from from 1 through 10. The default value is 2.

### Modes

Interface configuration mode

### Usage Guidelines

The **no** form of the command disables this functionality.

### Examples

The following example configures the device to retransmit an EAP-request/challenge frame to a client a maximum of three times.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x max-req 3
```

Release version	Command history
16r.1.00	This command was introduced.

# dot1x port-control

Controls port-state authorization and configures the port control type to activate authentication on an 802.1X-enabled interface.

## Syntax

```
dot1x port-control { auto | force-authorized | force-unauthorized }
```

```
no dot1x port-control { auto | force-authorized | force-unauthorized }
```

## Command Default

The default port state is **auto**.

## Parameters

### auto

Enables authentication on a port. It places the controlled port in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized. This activates authentication on an 802.1X-enabled interface. The controlled port remains in the authorized state until the Client logs off.

### force-authorized

Places the controlled port unconditionally in the authorized state, allowing all traffic to pass between the client and the authenticator. This also allows connection from multiple clients.

### force-unauthorized

Places the controlled port unconditionally in the unauthorized state, denying any traffic to pass between the client and the authenticator.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Before activating the authentication using the **dot1x port-control auto** command on a port, you must remove the configured static ACL and static VLANs, if any, from the port.

802.1x port authentication is not supported by LAG (Link Aggregation Group) or interfaces that participate in a LAG.

The **no** form of the command resets the port control type to the default state.

## Examples

The following example configures the interface to place the port unconditionally in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control auto
```

The following example configures the interface to place the controlled port unconditionally in the authorized state.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control force-authorized
```

The following example configures the interface to place the controlled port unconditionally in the unauthorized state.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control force-unauthorized
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x reauthenticate

Initiates 802.1X reauthentication on a specified interface.

## Syntax

```
dot1x reauthenticate interface ethernet slot/port
```

## Parameters

**interface ethernet** *slot/port*

Specifies a physical interface ethernet port in terms of slot number and port number.

## Modes

Privileged EXEC mode

## Examples

The following example initiates reauthentication of a client connected to physical interface 1/1:

```
device# dot1x reauthenticate interface ethernet 1/1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x reauthentication

Configure the device to periodically reauthenticate the clients connected to 802.1X-enabled interfaces at regular intervals.

## Syntax

**dot1x reauthentication**

**no dot1x reauthentication**

## Command Default

Periodic reauthentication is disabled.

## Modes

Interface configuration mode

## Usage Guidelines

When periodic reauthentication is enabled using the **dot1x reauthentication** command, the device reauthenticates the clients every 3,600 seconds by default.

The reauthentication interval is configurable using the **dot1x timeout re-authperiod** command. The reauthentication interval configured using the **dot1x timeout re-authperiod** command takes precedence.

The **no dot1x reauthentication** command disables periodic reauthentication.

## Examples

The following example enables 802.1x reauthentication.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x reauthentication
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x reauthMax

Sets the maximum number of times that a port attempts 802.1x reauthentication before the port changes to the unauthorized state.

## Syntax

`dot1x reauthMax number`

`no dot1x reauthMax`

## Command Default

The number of times that a port attempts 802.1x authentication is 2.

## Parameters

*number*

Specifies the maximum number of reauthentication attempts before the port goes to the unauthorized state. Valid values range from 1 through 10.

## Modes

Interface configuration mode

## Usage Guidelines

The `no dot1x reauthMax` command restores the default setting.

## Examples

The following example sets the maximum number of reauthentication attempts to 5.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x reauthMax 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# dot1x quiet-period

Configures the time interval that the device remains idle between a failed authentication and a reauthentication attempt.

## Syntax

`dot1x quiet-period seconds`

`no dot1x quiet-period`

## Command Default

The default quiet period is 60 seconds.

## Parameters

*seconds*

Specifies the time between failed reauthentication and reauthentication attempt. Valid values range from 1 through 65535 seconds.

## Modes

Interface configuration mode

## Usage Guidelines

Changing the quiet-period interval time to a number lower than the default can result in a faster response time.

The `no dot1x quiet-period` command restores the default setting.

## Examples

The following example sets the idle time as 200 seconds for the device before attempting reauthentication after an authentication failure.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x quiet-period 200
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x test eapol-capable

Executes the 802.1x readiness check on the switch.

## Syntax

```
dot1x test eapol-capable interface ethernet slot/port
```

## Parameters

**interface ethernet** *slot/port*

Specifies a physical interface ethernet port in terms of slot number and port number.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is designated as 802.1x-capable.

The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). The readiness check is not available on a port that is configured with the command **dot1x port-control force-unauthorized**.

The readiness check is typically used before 802.1x is enabled on the switch.

802.1x authentication cannot be initiated while the 802.1x readiness test is in progress.

The 802.1x readiness test cannot be initiated while 802.1x authentication is active.

802.1x readiness can be checked on a per-interface basis. Readiness check for all interfaces at once is not supported.

## Examples

The following example configures readiness check on an interface to determine if the devices connected to the ports are 802.1x-capable.

```
device# dot1x test eapol-capable interface ethernet 1/1
device# 2016/07/18-00:49:03, [DOT1-1012], 5006, M2 | Active | DCE, INFO, sw0, DOT1X_PORT_EAPOL_CAPABLE:
Peer connected to port Ethernet 1/1 is EAPOL capable.
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x test timeout

Sets the 802.1X readiness test timeout.

## Syntax

`dot1x test timeout timeout`

## Command Default

The default readiness test interval is 10 seconds.

## Parameters

*timeout*

Specifies the readiness test interval value in seconds. Valid values range from 1 through 65535.

## Modes

Global configuration mode

## Examples

The following example sets the test timeout to 30 seconds:

```
device(config)# dot1x test timeout 30
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dot1x timeout

Configures the timeout parameters that determine the time interval for client reauthentication and EAP retransmissions.

## Syntax

```
dot1x timeout {re-authperiod seconds | supp-timeout seconds | tx-period seconds }
```

```
no dot1x timeout {re-authperiod seconds | supp-timeout seconds | tx-period seconds }
```

## Command Default

The timeout parameters are not applied to the device.

## Parameters

### re-authperiod *seconds*

Specifies the interval at which clients connected to 802.1X authentication enabled ports are periodically reauthenticated. When periodic reauthentication is enabled using the **dot1x reauthentication** command, the device reauthenticates the clients every 3,600 seconds by default. The **re-authperiod** option allows you to specify the time interval between reauthentication attempts. The reauthentication interval configured using the **dot1x timeout re-authperiod** command takes precedence.

### supp-timeout *seconds*

Specifies the EAP response timeout for 802.1x authentication. By default, when the device relays an EAP-Request frame from the RADIUS server to the client, it expects to receive a response from the client within 30 seconds. If the client does not respond within the allotted time, the device retransmits the EAP-Request frame to the client. The timeout value for retransmission of EAP-Request frames to the client can be configured using the **supp-timeout seconds** parameters.

### tx-period *seconds*

Specifies the EAP request retransmission interval, in seconds, with the client. By default, if the device does not receive an EAP-response/identity frame from a client, the device waits 30 seconds, then retransmits the EAP-request/identity frame. You can optionally change the amount of time the device waits before re-transmitting the EAP-request/identity frame to the client. If the client does not send back an EAP-response/identity frame within 60 seconds, the device will transmit another EAP-request/identity frame. The tx-period is a value from 1 through 4294967295. The default is 30 seconds.

## Modes

Interface configuration mode

## Usage Guidelines

The **no** form of the command disables dot1x timeout.

## Examples

The following example sets 25 seconds as the amount of time between reauthorization attempts on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout re-authperiod 25
```

The following example sets 45 seconds as the switch-to-client retransmission time for the EAP request frame on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout supp-timeout 45
```

The following example sets 34 seconds as the waiting period for a response to an EAP-request or identity frame from the client before retransmitting the request on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout tx-period 34
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dscp

Configures the tunnel differentiated services code point (DSCP).

## Syntax

```
dscp dscp-value
no dscp
```

## Parameters

*dscp-value*  
Specifies the DSCP value. The range is from 0 to 63.

## Command Default

The default value is 0.

## Modes

Interface tunnel configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the DSCP configuration.

## Examples

This example configures DSCP value for the tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
device(config-intf-tunnel-5)# dscp 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# dscp-ttl-mode

Configures tunnel differentiated services code point (DSCP) time to live (TTL) mode.

## Syntax

```
dscp-ttl-mode { pipe | uniform }
no dscp-ttl-mode
```

## Command Default

By default, set to pipe mode for all tunnels.

## Parameters

**pipe**  
Specifies pipe mode.

**uniform**  
Specifies uniform mode.

## Modes

Interface tunnel configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the QoS mode configuration.

Supporting the QoS mutation configuration on the VE is not supported.

## Examples

This example shows how to configure the quality of service (QoS) mode.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
```

## History

Release version	Command history
16r.1.00	This command was introduced.





# Commands E - F

---

## ebs

Configures the excess burst size of a class map.

## Syntax

**ebs** *ebs-size*

**no ebs** *ebs-size*

## Parameters

*ebs-size*

Excess burst size. Valid values range from 1250 through 12500000000 bytes in increments of 1 byte.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **ebs** commands are mandatory for configuring a class map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete parameters for a class map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** version of this command to remove the parameter from the class map.

## Examples

This example configures a class-map called "default" within a policy map.

```
device# configure terminal
device(config)# policy-map policymap1
device(config-policymap)# class default
device (config-policymap-class)# police cir 40000
device(config-policymap-class-police)# ebs 400000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## eir

Configures the excess information rate for a class map.

## Syntax

**eir** *eir-rate*

**no eir** *eir-rate*

## Parameters

*eir-rate*

Excess information rate. Valid values range from 0 through 300000000000 bps.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete parameters for a class map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** form of this command to remove the parameter from the class map.

## Examples

This example configures a class map called "default" within a policy map.

```
device# configure terminal
device(config)# policy-map policymap1
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
device(config-policymap-class-police)# eir 1200000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# enforce-first-as

Enforces the use of the first autonomous system (AS) path for external BGP (EBGP) routes.

## Syntax

**enforce-first-as**

**no enforce-first-as**

## Command Default

This option is disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

This command causes the router to discard updates received from EBGP peers that do not list their AS number as the first AS path segment in the AS\_PATH attribute of the incoming route.

## Examples

This example configures the device to enforce the use of the first AS path.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# enforce-first-as
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# eol

Enables the end-of-lib configuration mode.

## Syntax

```
eol
no eol
```

## Modes

MPLS LDP configuration mode

## Usage Guidelines

Use the **no** form of this command to remove this mode and attribute under it.

The end-of-lib mode contains all the attributes of the end of lib capability and notification. Also, when you enable the end-of-lib mode, you can determine whether the two RFCs 5561 and 5919 are enabled by the LSR.

## Examples

The following example enables the end-of-lib configuration mode.

```
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# eol
device(config-router-mpls-ldp-eol)#
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# error-disable-timeout enable

Enables the timer to bring the interface out of the error-disabled state.

## Syntax

**error-disable-timeout enable**

## Modes

Spanning tree configuration mode

## Usage Guidelines

When the Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) guard disables a port, the port remains in the disabled state unless the port is enabled manually. This command allows you to enable the interface from the disabled state.

The command is the same regardless of which type of STP is enabled.

## Examples

To bring the interface out of the disabled state:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree rpvt
device(conf-rpvst)# error-disable-timeout enable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# error-disable-timeout interval

Sets the timeout interval for errors on an interface.

## Syntax

```
error-disable-timeout interval seconds
no error-disable-timeout interval
```

## Command Default

300 seconds

The timeout feature is disabled.

## Parameters

*seconds*

Specifies the time for the interface to time out. Valid values range from 10 through 1000000 seconds.

## Modes

Spanning tree configuration mode

## Usage Guidelines

Enter **no error-disable-timeout interval** to return to the default setting.

The command is the same regardless of which type of STP is enabled.

## Examples

Follow these examples to set the timeout interval.

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# error-disable-timeout interval 100
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# error-disable-timeout interval 100
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# error-disable-timeout interval 100
```

```
device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# error-disable-timeout interval 100
```

```
device# configure terminal
device(config)# protocol spanning-tree rpvt
device(conf-rpvst)# error-disable-timeout interval 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## esi

Sets the Ethernet Segment ID (ESI) value which is used to uniquely identify the cluster clients.

## Syntax

**esi** *HH:HH:HH:HH:HH:HH:HH:HH:HH*

**no esi** *HH:HH:HH:HH:HH:HH:HH:HH:HH*

## Parameters

*HH:HH:HH:HH:HH:HH:HH:HH:HH*

Specifies the 9-octet ESI value. Enter *HH* in hexadecimal format.

## Modes

Cluster client configuration mode

## Usage Guidelines

Use the **no** form of the command to delete the ESI setting.

Configure the same value on both MCT devices to create the MCT client LAG.

The same ESI cannot be added under multiple client entries.

## Examples

The following example shows the setting of the ESI for the cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# esi 00.a1.b2.c3.d4.e5.f6.89.00
```

## History

Release version	Command history
16r.1.01	This command was introduced.



# event-handler

Creates or accesses an event-handler profile, which can execute a Python script when a specified trigger occurs. You can optionally specify a description, a trigger, or the Python script with this command; or specify them later.

## Syntax

```
event-handler event-handler-name [ action python-script file-name ]
```

```
event-handler event-handler-name [ trigger trigger-id [ raslog raslog-id ] ]
```

```
no event-handler event-handler-name
```

## Command Default

No event-handler profile is enabled.

## Parameters

*event-handler-name*

Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

**action** **python-script** *file-name*

Specifies a Python file that runs when a trigger-condition occurs. Valid values range from 4 through 32 characters (including the **.py** extension). The first character must be alphanumeric.

**trigger** *trigger-id*

Defines an event-handler trigger and specifies an ID number for the trigger. Valid values are 1 through 100, and must be unique per event-handler profile. When the trigger-condition occurs, a Python script is run.

**raslog** *raslog-id*

Specifies a RASlog message ID as the trigger.

## Modes

Global configuration mode

Event-handler configuration mode for an existing event handler. (There is no need to enter the **exit** command to return to global configuration mode.)

## Usage Guidelines

You can create multiple event-handler profiles.

An **event-handler** command creates or accesses an event-handler profile and can also define one of the following parameters:

- One trigger
- The Python-script action that runs on any trigger

You can also define the above parameters—including one or more triggers—from event-handler configuration mode.

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

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

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

## Examples

The following example creates an event-handler profile and accesses its configuration mode.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# clear event-handler action

Under Python event-management, aborts a specified event handler that is currently running.

## Syntax

```
clear event-handler action event-handler-name
```

## Parameters

*event-handler-name*

Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

## Modes

Privileged EXEC mode

## Examples

The following command successfully aborted event-handler action "eh1".

```
device# clear event-handler action eh1
This operation will abort an event handler action that is currently running and may leave the device in
an inconsistent state. Do you want to continue? [y/n]:y
Operation completed successfully.
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# event-handler activate

Activates an event handler and accesses event-handler activation mode, from which you can enter advanced configuration commands. You can also append the advanced commands to **event-handler activate**.

## Syntax

**event-handler activate** *event-handler-name*

**event-handler activate** *event-handler-name* [ **delay** *seconds* ] [ **iterations** *num-iterations* ] [ **interval** *seconds* ] [ **trigger-mode** *mode* ] [ **trigger-function** { **OR** | **AND** [ **time-window** *seconds* ] } ]

**no event-handler activate** *event-handler-name*

## Command Default

No event handler is activated on the device.

## Parameters

*event-handler-name*

Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

**delay** *seconds*

Specifies a number of seconds from when a trigger is received until the execution of the specified action begins. Valid values are 0 or a positive integer.

**iterations** *num-iterations*

Specifies the number of times an event-handler action is run, when triggered. Valid values are any positive integer. The default value is 1.

**interval** *seconds*

Specifies the number of seconds between iterations of an event-handler action, if triggered. Valid values are 0 or a positive integer. The default is 0.

**trigger-mode** *mode*

Specifies if an event-handler action can be triggered only once or more than once. The default is each time the trigger condition occurs, the event-handler action is launched.

**each-instance**

The event-handler action is launched on each trigger instance received.

**on-first-instance**

As long as the device is running, the event-handler action is launched only once. Following a device restart, the event-handler action can be triggered again.

**only-once**

For the duration of a device's configuration, the event-handler action is launched only once.

**trigger-function**

For an implementation of an event-handler profile, if multiple triggers are defined for an event-handler action, specifies if the action runs only if all of the triggers occur; or if one is sufficient.

**OR**

The event-handler action runs if any of the triggers occur.

**AND**

The event-handler action runs only if all of the triggers occur.

**time-window** *seconds*

In seconds, specify the time window within which all of the triggers must occur in order that the event-handler action runs. Once all triggers have been received and on each subsequent trigger received, the action will be launched when the time difference between the latest trigger and the oldest trigger is less than or equal to the configured time-window.

Following an initial triggering of an event-handler action, any subsequent trigger launches the action an additional time if the following conditions are true:

- The **trigger-mode** parameter is set to the default **each-instance**.
- The subsequent trigger occurs within the specified **time-window**.

## Usage Guidelines

You can activate up to 10 different event-handler profiles on a device.

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

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

For additional usage guidelines regarding the advanced configuration commands, see the following topics:

- **delay**
- **iterations**
- **interval**
- **run-mode**
- **trigger-mode**
- **trigger-function**

To inactivate an event-handler instance on a device, use the **no** form of this command. If an event-handler Python script is running, it is executed to completion before inactivation of the event handler.

## Examples

This example activates eventHandler1 on the device.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# exceed-set-dscp

Configures the CIR packet IP precedence of a class map.

## Syntax

```
exceed-set-dscp dscp-num
```

```
no exceed-set-dscp dscp-num
```

## Parameters

*dscp-num*

Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and sent to the EIR bucket will have packet IP precedence set to the value in the *dscp-num* variable. Valid values are 0 through 7.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** version of this command to remove the parameter from the class map.

## Examples

Example of setting this parameter.

```
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
device(config-policymap-class-police)# exceed-set-dscp 4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# exceed-set-prec

Configures the CIR packet IP precedence of a class-map.

## Syntax

**exceed-set-prec** *prec-num*

**no exceed-set-prec** *prec-num*

## Parameters

*prec-num*

Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and sent to the EIR bucket will have packet IP precedence set to the value in the *prec-num* variable. Valid values are 0 through 7.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete parameters for a class map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** version of this command to remove the parameter from the class-map.

## Examples

Example of setting this parameter.

```
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
device(config-policymap-class-police)# exceed-set-prec 4
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# exceed-set-tc

Configures the queue assignment of the *trafficclass* variable for a class map.

## Syntax

**exceed-set-tc** *trafficclass*

**no exceed-set-tc** *trafficclass*

## Parameters

*trafficclass*

Specifies that traffic with bandwidth requirements that exceed the rate configured for CIR and is in the limit of what is configured for EIR will have its traffic class (internal queue assignment) set to the value in the *trafficclass* variable. Valid values are 0 through 7.

## Modes

Policy map class police configuration mode

## Usage Guidelines

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete parameters for a class map, you must delete all policer parameters while in the policy map class configuration mode using the **no police cir** command.

Use the **no** version of this command to remove the parameter from the class map.

## Examples

Example of setting this parameter.

```
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
device(config-policymap-class-police)# exceed-set-tc 4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# external-lsdb-limit (OSPFv2)

Configures the maximum size of the external link state database (LSDB).

## Syntax

```
external-lsdb-limit value
no external-lsdb-limit
```

## Command Default

14913080

## Parameters

*value*

Maximum size of the external LSDB. Valid values range from 1 through 14913080.

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

If you change the value, make sure to save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

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

## Examples

The following example sets the limit of the LSDB to 20000.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# external-lsdb-limit 20000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# external-lsdb-limit (OSPFv3)

Configures the maximum size of the external link state database (LSDB).

## Syntax

```
external-lsdb-limit value
no external-lsdb-limit
```

## 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-ipv6-router-ospf-vrf-default-vrf)# external-lsdb-limit 15000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## exclude-any

Interfaces that are not part of these groups, as well as interfaces that are not part of any group, are eliminated from consideration.

### Syntax

```
exclude-any {[ name |number ]}
no exclude-any {[ name |number ]}
```

### Command Default

There are no excluded interfaces in the command default mode.

### Parameters

*name*  
Specifies the group, by name, to exclude.

*number*  
Specifies the group, by number, to exclude.

### Modes

MPLS LSP configuration mode (config-router-mpls lsp-*lsp\_name* ).

### Usage Guidelines

The **no** form of the command removes the interface administrative group configuration.

More than one group may be configured at a time.

### Examples

The following example excludes interfaces in either administrative group "gold" or "silver" when the path for LSP *tunnel1* is calculated.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# exclude-any gold silver
```

### History

Release version	Command history
16r.1.00	This command was introduced.

# fast-external-fallover

Resets the session if a link to an eBGP peer goes down.

## Syntax

```
fast-external-fallover
no fast-external-fallover
```

## 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 convergence time, but can also lead to instability in the BGP routing table as a result of a flapping interface.

## Examples

This example configures the device to reset the session if a link to an eBGP peer goes down.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# fast-external-fallover
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# fast-flood

Configures Intermediate System-to-Intermediate System (IS-IS) to flood Link State PDUs to other devices in the network before running SPF.

## Syntax

**fast-flood** *lsp-count*

**no fast-flood** *sp-count*

## Command Default

Four LSPs are flooded before running SPF.

## Parameters

*lsp-count*

Specifies the number of LSPs that must be flooded before running SPF. Valid values range from 1 through 15. The default value is 4.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command resets the LSP count to the default value of 4.

## Examples

The following example configures IS-IS to flood 10 LSPs before running SPF.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# fast-flood 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# fastboot

Reboots the management module on which the command is executed.

## Syntax

**fastboot**

## Modes

Privileged EXEC mode

## Usage Guidelines

All reboot operations are disruptive, and the commands prompt for confirmation before executing. When you reboot a device, all traffic to and from it stops. All ports on that device remain inactive until the device comes back online.

Any unsaved configurations are lost.

If you log in to the device IP address and enter this command, only the active management module reboots and POST is bypassed.

## Examples

The following example shows the use of the **fastboot** command.

```
device# fastboot
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# filter-fec-in

Configures LDP inbound or outbound FEC filtering to filter inbound label bindings on a MPLS router.

## Syntax

**filter-fec-in** *prefix-list-name*

**no filter-fec-in** *prefix-list-name*

## Command Default

By default, LDP distributes all FECs that are learned locally or from LDP neighbors to all other LDP neighbors.

## Parameters

*prefix-list-name*

Specifies the prefix-list name.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the FEC filtering configuration.

LDP inbound-FEC filtering allows the control the amount of memory and CPU processing involved in installing and advertising label bindings not used for forwarding. It also serves as a tool to avoid DOS attack. For inbound FEC filter, consider the following:

- The FECs filtered by the LDP inbound-FEC filter do not install in the forwarding plane or advertise to the upstream neighbors. The FEC remains in the retained state.
- The LDP inbound-FEC filter are changed directly without deleting the one previously configured. The change automatically applies and triggers the filtering of inbound FECs.
- Changes to a referenced prefix-list automatically applies to LDP inbound-FEC filtering. This triggers filtering by way of the new configuration, filtering any existing FECs which violate the filter.
- To allow multiple route filter updates, the device waits for default 10 seconds before notifying the application of the filter change. The time for notification is configurable.
- When the LDP inbound-FEC filter is not configured, LDP does not filter any inbound FECs.
- By default, when the prefix-list referenced by the LDP inbound-FEC filter has no configuration, it is an implicit deny. All inbound FECs are filtered out and retained. The behavior is the same when the prefix list is deleted after setting it in the inbound FEC filter configuration. This behavior is consistent with other protocols which use device filters and also with the use of the **advertise-fec** command for LDP route injection.
- Inbound FEC filtering is applicable only for Layer 3 FECs and not for VC FECs. Inbound FEC filtering is not applicable for Layer 2 VPNs.



## Examples

The following example configures the LDP inbound-FEC filter.

```
device# configure terminal
device(config)# ip prefix-list list-abc permit 10.20.20.0/24
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# filter-fec-in list-abc
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# filter-fec-out

Configures LDP outbound FEC filtering to filter outbound label bindings on a MPLS router.

## Syntax

**filter-fec-out** *prefix-list-name*

**no filter-fec-out** *prefix-list-name*

## Command Default

By default, LDP distributes all FECs that are learned locally or from LDP neighbors to all other LDP neighbors.

## Parameters

*prefix-list-name*

Specifies the prefix-list name.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the FEC filtering configuration.

LDP outbound FEC filtering gives you the ability to control which FECs can be advertised and to which LDP neighbors. It also reduces the number of labels distributed to neighbors and the number of messages exchanged with peers. Through this filtering, LDP scalability and convergence, security, and performance are improved.

## Examples

The following example configures the LDP outbound-FEC filter.

```
device# configure terminal
device(config)# ip prefix-list list-out deny 10.40.40.0/24
device(config)# ip prefix-list list-out permit 0.0.0.0/0 ge 32
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# filter-fec-out list-out
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# forward-delay

Specifies the time an interface spends in each of the listening and learning states.

## Syntax

**forward-delay** *seconds*

**no forward-delay**

## Command Default

15 seconds

## Parameters

*seconds*

Specifies the time that an interface spends in the Spanning Tree Protocol (STP) learning and listening states. Valid values range from 4 through 30 seconds.

## Modes

Spanning tree configuration mode

## Usage Guidelines

This command specifies how long the listening and learning states last before the interface begins the forwarding of all spanning-tree instances.

STP interface states:

- Listening - The interface processes the Bridge Protocol Data Units (BPDUs) and awaits possible new information that might cause it to return to the blocking state.
- Learning - The interface does not yet forward frames (packets), instead it learns source addresses from frames received and adds them to the filtering database (switching database).
- Forwarding - An interface receiving and sending data, normal operation. STP still monitors incoming BPDUs that can indicate it should return to the blocking state to prevent a loop.
- Blocking - An interface that can cause a switching loop, no user data is sent or received, but it might go to the forwarding state if the other links in use fail and the STP determines that the interface may transition to the forwarding state. BPDU data continues to be received in the blocking state.

When you change the spanning-tree forward-delay time, it affects all spanning-tree instances. When configuring the forward-delay, the following relationship should be kept:

$$(2 \times (\text{forward-delay} - 1)) \geq \text{max-age} \geq (2 \times (\text{hello-time} + 1))$$

Enter **no forward-delay** to return to the default settings.

The command is the same regardless of which type of STP is enabled.

## Examples

To configure the forward-delay time to 18 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# forward-delay 18
```

```
device# configure terminal
device(config)## protocol spanning-tree rstp
device(conf-rstp)# forward-delay 18
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# forward-delay 18
```

```
device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# forward-delay 18
```

```
device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# forward-delay 18
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# from

Configures only the local interface of the routing device. The command penalizes any link on the specified interface, but not all links when the link is a multi-access link.

## Syntax

```
from { ip_addr }
no from { ip_addr }
```

## Command Default

The command is disabled, by default.

## Parameters

*ip\_addr*  
Specifies the selected IP address of the fate sharing group

## Modes

MPLS CSPF-group configuration mode.

## Usage Guidelines

The order in which the local IP address to the remote IP address is configured is insignificant. For example, the configuration from 10.10.10.10 to 10.20.20.20 and from 10.20.20.20 to 10.10.10.10 has the same meaning.

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

## Examples

The following example configures the local address *10.1.1.1* of the fate sharing group.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# cspf-group group3
device(config-router-mpls-cspf-group-group3)# from 10.1.1.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# Commands G - J

---

## graceful-restart (BGP)

Enables the BGP graceful restart capability.

### Syntax

```
graceful-restart [ purge-time seconds | restart-time seconds | stale-routes-time seconds ]
```

```
no graceful-restart
```

### Command Default

Disabled.

### Parameters

#### purge-time

Specifies the maximum period of time, in seconds, for which a restarting device maintains stale routes in the BGP routing table before purging them. The default value is 600 seconds. The configurable range of values is from 1 to 3600 seconds.

#### restart-time

Specifies the restart-time, in seconds, advertised to graceful restart-capable neighbors. The default value is 120 seconds. The configurable range of values is from 1 to 3600 seconds.

#### stale-routes-time

Specifies the maximum period of time, in seconds, that a helper device will wait for an End-of-RIB (EOR) message from a peer. All stale paths are deleted when this time period expires. The default value is 360 seconds. The configurable range of values is from 1 to 3600 seconds.

### Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use this command under a BGP address-family configuration mode to enable or disable the graceful-restart capability for all BGP neighbors in the address family. When this command is enabled, graceful-restart capability is negotiated with neighbors in the BGP OPEN message when a session is established. If the neighbor advertises support for graceful restart, that function is activated for that neighbor session. Otherwise, graceful restart is not activated for that session, even though it is enabled locally. If the neighbor has not sent graceful-restart parameters, the restarting device will not wait for the neighbor to start route calculation, but graceful restart will be enabled.

If the graceful-restart capability is enabled after a BGP session has been established, the neighbor session must be cleared for graceful restart to take effect.

The **purge-time** parameter is applicable for both restarting and helper devices. The timer starts when a BGP connection is closed. The timer ends when an EOR is received from all nodes, downloaded into BGP and an EOR sent to all neighbors. The configured purge-time timer value is effective only on the configured node.

The **restart-time** parameter is applicable only for helper devices. The timer starts at the time the BGP connection is closed by the remote peer and ends when the Peer connection is established. The configured restart-time timer value is effective only on the peer node, and not in the configured node. During negotiation time, the timer value is exchanged.

The **stale-routes-time** parameter is applicable only for helper devices. The timer starts when the peer connection is established after the HA-failover. The timer ends at the time an EOR is received from the peer. The configured stale-time timer value is effective only on the configured node.

For non-default VRF instances, graceful restart timers are inherited from the default VRF. The **purge-time**, **restart-time**, and **stale-routes-time** parameters are not available in BGP address-family IPv4 unicast VRF configuration mode and BGP address-family IPv6 unicast VRF configuration mode.

Use the **clear ip bgp neighbor** command with the **all** parameter for the changes to the graceful-restart parameters to take effect immediately.

The **no** form of the command disables the BGP graceful-restart capability globally for all BGP neighbors in the address family.

## Examples

The following example enables the BGP graceful restart capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
```

The following example sets the purge time to 240 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart purge-time 240
```



The following example sets the restart time to 60 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart restart-time 60
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sets the stale-routes time to 180 seconds.

```
device# configure terminal
device(config)# rrouter bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1000::1 remote-as 2
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 1000::1 activate
device(config-bgp-ipv6u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv6u)# graceful-restart stale-routes-time 180
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# graceful-restart (LDP)

Enables the MPLS LDP graceful restart capability for all LDP sessions and accesses the graceful restart (GR) configuration mode .

## Syntax

```
graceful-restart
no graceful-restart
```

## Command Default

Disabled.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

When you enable LDP GR, the router waits until it receives an LDP Initialization message from its neighbor to know whether it must delete its states or start the LDP GR recovery procedure. It is applicable to all LDP sessions regardless of the adjacency type exists between the neighbors.

The **no** form of the command disables the LDP graceful-restart capability globally for all LDP sessions and removed the configuration.

## Examples

The following example enables the BGP graceful restart capability.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# graceful-restart (OSPFv2)

Enables the OSPF Graceful Restart (GR) capability.

## Syntax

```
graceful-restart [ helper-disable | restart-time seconds ]  
no graceful-restart
```

## Command Default

Graceful restart and graceful restart helper capabilities are enabled.

## Parameters

### helper-disable

Disables the GR helper capability.

### restart-time

Specifies the maximum restart wait time, in seconds, advertised to neighbors. The default value is 120 seconds. The configurable range of values is from 10 through 1800 seconds.

## Modes

OSPF router configuration mode

OSPF router VRF configuration mode

## Usage Guidelines

Use **no graceful-restart helper-disable** to re-enable the GR helper capability.

The **no** form of the command disables the graceful restart capability.

## Examples

The following example disables the GR helper capability.

```
device# configure terminal  
device(config)# router ospf  
device(config-router-ospf-vrf-default-vrf)# graceful-restart helper-disable
```

The following example re-enables the GR helper capability.

```
device# configure terminal  
device(config)# router ospf  
device(config-router-ospf-vrf-default-vrf)# no graceful-restart helper-disable
```

The following example re-enables the GR capability and changes the maximum restart wait time from the default value to 240 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# graceful-restart restart-time 240
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# graceful-restart helper (OSPFv3)

Enables the OSPFv3 graceful restart (GR) helper capability.

## Syntax

```
graceful-restart helper { disable | strict-lsa-checking }
no graceful-restart helper
```

## Command Default

GR helper is enabled.

## Parameters

### disable

Disables the OSPFv3 GR helper capability.

### strict-lsa-checking

Enables the OSPFv3 GR helper mode with strict link-state advertisement (LSA) checking.

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

The **no** form of the command disables the GR helper capability on a device.

## Examples

The following example enables GR helper and sets strict LSA checking.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# graceful-restart helper strict-lsa-checking
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# graceful-restart helper-disable (IS-IS)

Disables and enables Intermediate System-to-Intermediate System (IS-IS) graceful restart (GR) helper mode.

## Syntax

```
graceful-restart helper-disable
no graceful-restart helper-disable
```

## Command Default

The GR helper is enabled by default.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command re-enables the GR helper if it has been disabled.

## Examples

The following example disables the IS-IS GR helper.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# graceful-restart helper-disable
```

The following example re-enables the IS-IS GR helper.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no graceful-restart helper-disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# handle-isis-neighbor-down

Globally enables the handling of an IGP neighbor down event by MPLS. This command can be executed on the fly and takes effect immediately. It makes it possible to enable handling of neighbor down events for IS-IS.

## Syntax

```
handle-isis-neighbor-down
```

```
no handle-isis-neighbor-down
```

## Command Default

By default, RSVP does not handle IGP neighbor down events. RSVP IGP synchronization must be enabled to handle an IGP neighbor down event.

## Modes

MPLS policy mode (config-router-mpls-policy).

## Usage Guidelines

### Limitations

1. The **handle-isis-neighbor-down** command is independent of MPLS traffic engineering configurations. The **handle-isis-neighbor-down** command allows MPLS (RSVP) to handle IGP neighbor down events and take action, such as tearing down the associated RSVP sessions. For example, when IS-IS is configured as MPLS TE protocol, the user can still configure MPLS to handle an OSPF neighbor down event (and vice versa).
2. An IGP neighbor down event is handled only by the RSVP sub-component of MPLS by tearing down the associated sessions. This event is not handled by LDP sub-component of MPLS.
3. MPLS RSVP does not keep track of the current state of IGP neighbor. That is, when an IGP neighbor goes down, RSVP tears down all the associated sessions. But RSVP does not prevent bringing up any session while the IGP neighbor to RSVP next-hop is down (or not yet available). That is, the RSVP session is brought up even when the IGP neighbor to the next-hop does not exist.
4. An IGP neighbor down is treated as upstream neighbor down or downstream neighbor down event by RSVP, depending upon the direction of the LSP. When a downstream IGP neighbor goes down, it results in an LSP tear down or FRR switchover, whichever is applicable.
5. MPLS receives and processes an IGP neighbor down event only for the cases when an IGP neighbor goes down because of hellos not received from the peer.
6. When an IGP neighbor goes down because of an underlying interface down, MPLS does not react to an IGP neighbor down event as RSVP would also receive the interface down event and tears down associated LSP sessions. Handling an IGP neighbor down event is redundant in such situations.
7. When BFD is configured on IGP interfaces, an IGP neighbor down is detected quickly and may help RSVP converge faster.

8. When an IGP neighbor is Nonstop Routing or Graceful Restart (NSR/GR) capable, MPLS does not receive a neighbor down event when NSR is performed on the peer IGP router.
9. Faster FRR feature is not be triggered when MPLS detects that IGP neighbor is down. Instead, each FRR LSP is processed individually to perform local repair.
10. It is highly recommended to observe extreme caution when implementing this feature when BFD is enabled for the underlying IGP. Under some circumstances, unnecessary flapping for RSVP sessions/LSPs can occur with this combination.

The **no** version of the command does not handle IGP neighbor down events.

## Examples

The following example shows how to enable the RSVP to handle IGP neighbor down events for IS-IS.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# handle-isis-neighbor-down
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ha chassisreboot

Performs a reboot of the chassis.

## Syntax

```
ha chassisreboot
```

## Modes

Privileged EXEC mode

## Usage Guidelines

This command reboots the entire chassis. Both the active and the standby management module reboot. Both management modules retain their original high-availability (HA) role after the system comes back up. If the power-on self test (POST) is enabled, it is executed when the system comes back up.

This command is supported only on the active management module. This command is not supported on the standby management module. Both management modules must be in sync for the HA reboot operation to succeed. Failover and reboots can be disruptive.

## Examples

To perform an HA reboot:

```
device# ha chassisreboot
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# ha disable

Disables the High Availability (HA) feature on a device.

## Syntax

```
ha disable
```

## Command Default

HA is disabled.

## Modes

Privileged EXEC mode

## Usage Guidelines

If the HA feature is already disabled, this command has no effect.

This command is supported only on the active management module.

This command is not supported on the standby management module.

Do not use this command unless instructed by Extreme Technical Support.

## Examples

To disable HA on a device:

```
device# ha disable
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# ha enable

Enables the High Availability (HA) feature on a device.

## Syntax

```
ha enable
```

## Command Default

HA is disabled.

## Modes

Privileged EXEC mode

## Usage Guidelines

If the HA feature is already enabled, this command has no effect. If the HA feature is disabled, this command enables it. The standby management process reboots as part of the process.

Running the command displays a warning message and prompts for confirmation before rebooting the management module.

You can also use this command to display the servers that are running the syslogd daemon and those that system messages are sent to. Servers are specified in the configuration database by IP address.

This command is supported only on the local management module.

This command is not supported on the standby management module.

Do not use this command unless instructed by Extreme Technical Support.

## Examples

To enable HA on a device:

```
device# ha enable
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# ha failover

Initiates a failover from the active to the standby management module (MM).

## Syntax

```
ha failover
```

## Modes

Privileged EXEC mode

## Usage Guidelines

This command forces a failover from the active to the standby MM. When the process completes, the former standby performs a warm recovery and takes over as the active MM. If the active and standby MMs are not synchronized, the command aborts.

## Examples

To perform a failover:

```
device# ha failover
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# ha sync start

This command is used to enable the high availability (HA) state synchronization.

## Syntax

```
ha sync start
```

## Modes

Privileged EXEC mode

## Examples

To enable HA synchronization:

```
device# ha sync start
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# ha sync stop

Disables high availability state synchronization on a device.

## Syntax

**ha sync stop**

## Command Default

Synchronization is enabled.

## Modes

Privileged EXEC mode

## Examples

To disable state synchronization:

```
device# ha sync stop
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# hardware

Accesses hardware configuration mode to access the connector, port-group, and profile configuration modes.

## Syntax

**hardware**

## Modes

Global configuration mode

## Examples

The following example shows the accessing of hardware configuration mode.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# hello (LLDP)

Sets the interval between LLDP hello messages

## Syntax

```
hello seconds
no hello
```

## Command Default

30 seconds

## Parameters

*seconds*  
Valid values range from 4 through 180 seconds.

## Modes

LLDP protocol and profile configuration modes

## Usage Guidelines

Enter **no hello** to return to the default setting.

The LLDP hello messages can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

## Examples

To set the time interval to 10 seconds between the transmissions:

```
device# configure terminal
device (config)# protocol lldp
device(conf-lldp)# hello ?
Possible completions:
<4-180>   Seconds[30 seconds]
device(conf-lldp)# hello 10
```

To set the time interval to 8 seconds between the transmissions for a specific LLDP profile:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# hello 8
device(config-profile-test1)#
```



## History

Release version	Command history
16r. 1.00	This command was introduced.

# hello (MPLS RSVP)

Enables RSVP Hello on all RSVP interfaces and configure the interval and tolerance.

## Syntax

```
hello [ interval seconds ] [tolerance number ]
no hello [ interval ] [tolerance ]
```

## Command Default

RSVP Hello is disabled on the device.

The default interval is 9 seconds.

The default tolerance is 3 unacknowledged RSVP Hello requests before timeout.

## Parameters

**interval** *seconds*

Specifies the interval in seconds between two RSVP Hello requests. Enter an integer from 1 to 60.

**tolerance** *number*

Specifies the number of unacknowledged RSVP Hello requests before timeout. Enter a number from 1 to 255.

## Modes

MPLS RSVP configuration mode

MPLS interface RSVP configuration mode

## Usage Guidelines

When you configure the interval and tolerance for the RSVP-TE Hello protocol globally, they are pushed to all MPLS interfaces when MPLS interface configurations are not present. In addition to these two parameters, you can configure the acknowledgments globally.

You can configure RSVP-TE Hello interval and tolerance on an MPLS interface. The interface configurations take precedence over global configurations.

By default, acknowledgments are not sent on the MPLS interface supporting RSVP Hello when no sessions are taken on the interface.



### CAUTION

**When disabling RSVP hello, disable it on both sides of the link at the same time to avoid bringing down all the RSVP sessions going over that link.**

Use the **no** command to disable RSVP Hello, or to reset the default interval or tolerance settings.

The **no hello** command on the MPLS interface sets the RSVP-TE Hello parameters to the globally configured RSVP Hello parameter values. If RSVP Hello is not configured globally, it disables the RSVP Hello on the MPLS interface. Executing this removes the configuration from the interface.

## Examples

The following example enables RSVP hello globally and configures the interval at 15 seconds and a tolerance of 8.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)# hello interval 15 tolerance 8
```

The following example enables RSVP hello on an MPLS interface and configures the interval at 20 seconds and a tolerance of 10.

```
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/12
device(config-router-mpls-interface-1/12)# rsvp
device(config-router-mpls-interface-1/12-rsvp)# hello interval 20 tolerance 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# hello (UDLD)

Sets the hello transmit interval.

## Syntax

**hello** *hundred\_milliseconds*

**no hello**

## Command Default

5 is the default value (500 milliseconds).

## Parameters

*hundred\_milliseconds*

Valid values range from 1 through 60 (in counts of 100 milliseconds).

## Modes

Unidirectional link detection (UDLD) protocol configuration mode

## Usage Guidelines

Use this command to set the time interval between the transmission of hello UDLD PDUs from UDLD-enabled ports.

Enter **no hello** to return to the default setting.

## Examples

To set the time interval to 2,000 milliseconds between hello UDLD PDU transmissions:

```
device# configure terminal
device(config)# protocol udld
device(config-udld)# hello 20
```

# hello-acknowledgements

Configures the MPLS RSVP-TE Hello to respond back with Hello ACKs to neighbors not carrying any RSVP sessions.

## Syntax

`hello-acknowledgements`

`no hello-acknowledgements`

## Command Default

By default, RSVP Hello acknowledgements are disabled.

## Modes

MPLS RSVP configuration mode

## Usage Guidelines

Use the **no** form of this command to reset the default behavior.

## Examples

The following example enables RSVP Hello acknowledgements.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)# hello-acknowledgements
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# hello-interval (LDP)

Sets the interval between LDP Hello messages for LDP sessions for LDP interfaces. These messages maintain LDP sessions between the device and its LDP peers.

## Syntax

```
hello-interval interval
no hello-interval interval
```

## Command Default

For an LDP interface configuration, the default value is the interval for the configured global LDP Hello messages.

## Parameters

*interval*  
Specifies the interval in seconds. Enter an integer from 1 through 32767.

## Modes

MPLS interface LDP configuration mode

## Usage Guidelines

Use this command to set the interval for LDP Link Hello messages that are multicast to all routers on the subnet.

When you configure the LDP link interval for an interface, it overrides the global interval.

When a Hello Adjacency already exists, the adjacency remains up and any new configured interval takes effect upon the expiration of the current Hello Interval timer. Consequently, the next and subsequent Hello messages are sent at the new interval.

Use the **no** for this command to reset the default interval.

## Examples

The following example sets the link Hello message interval for the interface to 30 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/2
device(config-router-mpls-interface-1/2)# ldp-params
device(config-router-mpls-interface-1/2-ldp-params)# hello-interval 30
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# hello-interval (PIM)

Sets the frequency with which the device sends PIM hello messages to its neighbors.

## Syntax

`hello-interval` *seconds*

`no hello-interval`

## Command Default

The default is 30 seconds.

## Parameters

*seconds*

Specifies the hello interval value in seconds. The range is 10 to 3600 seconds.

## Modes

PIM Router configuration mode

## Examples

The following example sets the PIM hello interval.

```
device(config)# router pim
device(config-pim-router)# hello-interval 50
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# hello-interval-link

Sets the interval between LDP link Hello messages globally which applies to all LDP interfaces. These messages are used to maintain LDP sessions between the device and its LDP peers.

## Syntax

```
hello-interval-link interval
no hello-interval-link
```

## Command Default

The default is 5 seconds.

## Parameters

*interval*

Specifies the interval in seconds. Enter an integer from 1 through 32767.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

Use this command to globally set the interval for LDP Link Hello messages that multicast to all routers on the subnet.

When you configure the LDP link interval for an interface, it overrides the global interval for the interface.

When a Hello Adjacency already exists, the adjacency remains up and any new configured interval takes effect upon the expiration of the current Hello Interval timer. Consequently, the next and subsequent hello messages are sent at the new interval.

Use the **no** for this command to reset the default interval.

## Examples

The following example sets the global interval to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-interval-link 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# hello-interval-target

Sets the interval between LDP Targeted Hello messages globally for all LDP interfaces. These messages are used to maintain LDP sessions between the device and its LDP peers.

## Syntax

**hello-interval-target** *interval*

**no hello-interval-target**

## Command Default

The default is 15 seconds.

## Parameters

*interval*

Specifies the interval in seconds. Enter an integer from 1 through 32767.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

Use this command to set the interval for LDP Targeted Hello messages that are unicast to a specific address, such as a VLL peer.

For targeted LDP sessions, the LDP Hello Interval can only be set globally.

Use the **no** for this command to reset the default interval.

## Examples

The following example sets the interval for LDP Targeted Hello messages to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-interval-target 10
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# hello-time

Sets the interval between the hello Bridge Protocol Data Units (BPDUs) sent on an interface.

## Syntax

**hello-time** *seconds*

**no hello-time**

## Command Default

2 seconds

## Parameters

*seconds*

Specifies the time interval between the hello BPDUs sent on an interface. Valid values range from 1 through 10 seconds.

## Modes

Spanning tree configuration mode

## Usage Guidelines

This command configures the spanning-tree bridge hello time, which determines how often the device broadcasts hello messages to other devices.

If the VLAN parameter is not provided, the **hello-time** value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration. When configuring the **hello-time**, the **max-age** command setting must be greater than the **hello-time** setting. The following relationship should be kept:

$$(2 \times (\text{forward-delay} - 1)) \geq \text{max-age} \geq (2 \times (\text{hello-time} + 1))$$

Enter **no hello-time** to return to the default settings.

The command is the same regardless of which type of STP is enabled.

## Examples

To configure spanning tree bridge hello time to 5 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# hello-time 5
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# hello-time 5
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# hello-time 5
```

```
device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# hello-time 5
```

```
device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# hello-time 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# hello-timeout (LDP)

Sets how long the device waits for its LDP peers for LDP sessions to send a Hello message for LDP interfaces.

## Syntax

**hello-timeout** *seconds*

**no hello-timeout** *seconds*

## Command Default

For an LDP interface configuration, the default value is the hold time for the configured global LDP Hello messages.

## Parameters

*seconds*

Specifies the hold time in seconds. Enter an integer from 2 through 65335. The minimum value that can be configured for the hold time is two times the value set for the Hello interval.

## Modes

MPLS interface LDP configuration mode

## Usage Guidelines

When the device does not receive a Hello message within this time, the LDP session with the peer can be terminated. The device includes the hold time in the Hello messages it sends out to its LDP peers.

The new time takes effect immediately and goes in the next Hello message sent. This hold time applies to only the hold time that the device sends to its peers. It does not affect the hold time the device uses to time out those peers. The latter is determined from the hold time that peers send to the device.

Use the **no** for this command to reset the default interval.

## Examples

The following example sets the link Hello hold time for the interface to 30 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/2
device(config-router-mpls-interface-1/2)# ldp-params
device(config-router-mpls-interface-1/2-ldp-params)# hello-timeout 30
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# hello-timeout-link

Sets how long the device waits for its LDP peers for link LDP sessions to send a Hello message.

## Syntax

`hello-timeout-link seconds`

`no hello-timeout-link`

## Command Default

The default is 15 seconds.

## Parameters

*seconds*

Specifies the hold time in seconds. Enter an integer from 2 through 65335.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

When the device does not receive a Hello message within this time, the LDP session with the peer can be terminated. The device includes the hold time in the Hello messages it sends out to its LDP peers.

The new time takes effect immediately and goes in the next Hello message sent. This hold time applies to only the hold time that the device sends to its peers. It does not affect the hold time the device uses to time out those peers. The latter is determined from the hold time that peers send to the device.

Use the **no** for this command to reset the default hold time.

## Examples

The following example sets the global hold time to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-timeout-link 10
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# hello-timeout-target

Sets how long the device waits for its LDP peers for targeted LDP sessions to send a Hello message.

## Syntax

**hello-timeout-target** *seconds*

**no hello-timeout-target**

## Command Default

The default is 45 seconds.

## Parameters

*seconds*

Specifies the hold time in seconds. Enter an integer from 2 through 65335.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

When the device does not receive a Hello message within this time, the LDP session with the peer can be terminated. The device includes the hold time in the Hello messages it sends out to its LDP peers.

The new time takes effect immediately and goes in the next Hello message sent. This hold time applies to only the hold time that the device sends to its peers. It does not affect the hold time the device uses to time out those peers. The latter is determined from the hold time that peers send to the device.

Use the **no** for this command to reset the default timeout.

## Examples

The following example sets the global hold time to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-timeout-target 10
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# hello padding

Re-enables the padding of Intermediate System-to-Intermediate System (IS-IS) hello Protocol Data Units (PDUs) globally.

## Syntax

```
hello padding [ disable ] [ point-to-point ]  
no hello padding [ disable ] [ point-to-point ]
```

## Command Default

Enabled.

## Parameters

**disable**  
Disables the padding of IS-IS hello PDUs.

**point-to-point**  
Specifies point-to-point interfaces.

## Modes

IS-IS router configuration mode

## Usage Guidelines

Generally, you do not need to disable padding unless a link is experiencing slow performance. If you enable or disable padding on an interface using the **isis hello padding** command, the interface setting overrides the global setting.

The **no** form of the command disables the padding of IS-IS hello PDUs.

## Examples

The following example globally disables padding of IS-IS hello PDUs.

```
device# configure terminal  
device(config)# router isis  
device(config-isis-router)# hello padding disable
```

The following example globally disables padding of IS-IS hello PDUs for point-to-point interfaces.

```
device# configure terminal  
device(config)# router isis  
device(config-isis-router)# hello padding disable point-to-point
```

The following example globally re-enables padding of IS-IS hello PDUs.

```
device# configure terminal  
device(config)# router isis  
device(config-isis-router)# hello padding
```

The following example globally re-enables padding of IS-IS hello PDUs for Point-to-Point interfaces.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hello padding point-to-point
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# helper-only

Specifies that the LSR acts as a helper only for LDP graceful restart.

## Syntax

**helper-only**

**no helper-only**

## Command Default

Full LDP GR mode with the router acting either as a restarting router or a GR helper.

## Modes

MPLS LDP GR configuration mode

## Usage Guidelines

A GR helper is an LSR whose neighbor is restarting its LDP component.

In helper mode, a router does not preserve its forwarding entries on a LDP GR restart. It indicates to its peers that forwarding state is not preserved by sending an initialization message with the Reconnect Time and the Recovery Time set to zero (0) in FT session TLV. The configuration commands for reconnect-time and recovery-time are rejected with informational messages. However, it can help a neighboring router recover its forwarding entries when the neighbor is going through restart.

The **no** form of the command removes the LDP GR helper mode and revert back to full LDP GR mode with the router acting either as a restarting router or a GR helper.

## Examples

The following example configures the LSR for LDP GR helper mode only.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# helper-only
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

## hold-time

Sets the time that a previously down backup VRRP router, which also must have a higher priority than the current master VRRP router, will wait before assuming mastership of the virtual router.

### Syntax

`hold-time range`

### Command Default

0 seconds

### Parameters

*range*

A value between 1 and 3600 seconds that specifies the time a formerly down backup router waits before assuming mastership of the virtual router.

### Modes

Virtual-router-group configuration mode

### Usage Guidelines

The hold-time must be set to a number greater than the default of 0 seconds for this command to take effect.

This command can be used for both VRRP and VRRP-E.

### Examples

To set the hold time to 60 seconds for backup routers in a specific virtual router:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# hold-time 60
```

### History

Release version	Command history
16r.1.00	This command was introduced.

# hop-limit

Gives the ability to change the hop limit to a lower number.

## Syntax

```
hop-limit { number }
```

```
hop-limit { number }
```

## Command Default

By default, the path calculated by CSPF can consist of no more than 255 hops, including the ingress and egress LERs.

## Parameters

*number*

Specifies the selected number of hops in the path. The range for the number of hops is 0 - 255 with a default number of 255.

## Modes

MPLS LSP configuration mode (*config-router-mpls-lsp-lsp\_name*).

## Usage Guidelines

The no for of the command roves the specified number of hops and returns to the default hop number of 255 hops.

## Examples

The following example limits the CSPF to choosing a path consisting of no more than 20 hops for LSP *tunnel1* .

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# hop-limit 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# hostname disable

Disables Intermediate System-to-Intermediate System (IS-IS) name mapping on a device.

## Syntax

```
hostname disable
no hostname disable
```

## Command Default

Disabled.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The implementation of IS-IS supports RFC 2763, which describes a mechanism for mapping IS-IS system IDs to the host names of the devices with those IDs. For example, if you set the host name on the device to "IS-IS Router 1", the mapping capability uses this name instead of the IS-IS system ID of the device in the output of the following commands:

- show isis database
- show isis interface
- show isis neighbor

The **no** form of the command re-enables IS-IS name mapping on a device.

## Examples

The following example disables IS-IS name mapping.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hostname disable
```

The following example re-enables IS-IS name mapping.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no hostname disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# implicit-commit

MPLS allows the user to modify the configurable parameters for RSVP LSPs while the LSP is operational.

## Syntax

```
implicit-commit { all | lsp-reoptimize-timer }
no implicit-commit
```

## Command Default

There is no implicit commit, by default.

## Parameters

**all**  
Enables an implicit commit for all triggers.

**lsp-reoptimize-timer**  
Enables an implicit commit for reoptimizations.

## Modes

MPLS policy configuration mode (config-router-mpls-policy).

## Usage Guidelines

The **no** form of the command removes the implicit commit.

After modifying the parameters for an operational LSP, the user must execute the **commit** command to apply the changes. Applying these configuration changes requires a new instance of the LSP to be signaled with a modified or new set of parameters, also known as make-before-break. Once the new instance of the LSP is up, the old instance is removed.

By default, if the adaptive parameters of an LSP have changed, but the changes are not yet committed, any system-initiated make-before-break, such as an LSP re-optimization event, is ignored. To allow changes to be automatically applied, the user can use the **implicit-commit lsp-reoptimize-timer** command under the router MPLS policy command to enable certain types of events to trigger implicit commit.

## Examples

The following example enable the LSP re-optimize timer to trigger an implicit commit.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# implicit-commit lsp-reoptimize-timer
```

Release version	Command history
16r.1.00	This command was introduced.

# inactivity-timer

Configures the time a forwarding entry can remain unused before the device deletes it.

## Syntax

`inactivity-timer seconds`

`no inactivity-timer seconds`

## Command Default

The default inactive time is 180 seconds.

## Parameters

*seconds*

Specifies the time in seconds. The range is 60 through 3600 seconds. The default is 180 seconds.

## Modes

PIM router configuration mode

## Usage Guidelines

The **no** form of this command restores the default inactive time, 180 seconds.

A device deletes a forwarding entry if the entry is not used to send multicast packets. The Protocol Independent Multicast (PIM) inactivity timer defines how long a forwarding entry can remain unused before the device deletes it.

## Examples

This example configures an inactive time to 90 seconds.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# inactivity-timer 90
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# include-all

When a device uses CSPF to calculate the path for an LSP, it takes into account the administrative group to which an interface belongs. The user can specify which administrative groups the device can include or exclude for this calculation.

## Syntax

```
include-all { [ name | number ] }
no include-all { [ name | number ] }
```

## Command Default

No interfaces are assigned to the administrative groups in the default mode.

## Parameters

*name*

Specifies the group, by name, the interface must be a member of.

*number*

Specifies the group, by number, the interface must be a member of.

## Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp\_name*).

## Usage Guidelines

Several administrative groups may be assigned to the LSP at the same time. The interface then must be a member of both groups.

The **no** form of the command removes the assigned interface.

## Examples

The following example specifies that the interface must be a member of both the "gold" and "silver" administrative groups to included in the path calculations for LSP *tunnel1*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# include-all gold silver
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# include-any

When a device uses CSPF to calculate the path for an LSP, it takes into account the administrative group to which an interface belongs. The user can specify which administrative groups the device can include or exclude for this calculation.

## Syntax

```
include-any { [ name | number ] }
no include-any { [ name | number ] }
```

## Command Default

No interfaces are assigned to the administrative groups in the default mode.

## Parameters

*name*  
Specifies the name of the selected administrative group.

*number*  
Specifies the number of the selected administrative group.

## Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp\_name* ).

## Usage Guidelines

The **no** form of the command removes the assigned interface.

Several administrative groups may be assigned to the LSP at the same time.

## Examples

The following example configures LSP *tunnel1* path calculations in either of the administrative groups "gold " or "silver ".

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# include-any gold silver
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ingress-tunnel-accounting

Excludes the Ethernet header (14 bytes) and Ethernet overhead (20 bytes) and CRC overhead (four bytes) when collecting byte statistics. In other words, it counts only the size of the MPLS packet.

## Syntax

`ingress-tunnel-accounting`

`no ingress-tunnel-accounting`

## Command Default

The command is disabled, by default.

## Modes

MPLS policy configuration mode.

## Usage Guidelines

To collect accurate statistics of the bypass LSP, it is necessary to configure ingress tunnel accounting at Label Switch Routers (LSR).

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

## Examples

The example below is a sample configuration for the command.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy) ingress-tunnel-accounting
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# install-igp-cost

Configures the device to use the IGP cost instead of the default BGP Multi-Exit Discriminator (MED) value as the route cost when the route is added to the Routing Table Manager (RTM).

## Syntax

```
install-igp-cost
no install-igp-cost
```

## 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-router)# install-igp-cost
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# instance

Maps a VLAN to a Multiple Spanning Tree Protocol (MSTP) instance. You can group a set of VLANs to an instance.

## Syntax

```
instance instance_id [ vlan vlan_id | priority priority_id ]
```

```
no instance
```

## Command Default

The priority value is 32768.

## Parameters

*instance\_id*

Specifies the MSTP instance. Valid values range from 1 through 31.

**vlan** *vlan\_id*

Specifies the VLAN to map an MSTP instance. Refer to the Usage Guidelines.

**priority** *priority\_id*

Specifies the priority for the specified instance. Valid values range from 0 through 61440. The priority values can be set only in increments of 4096.

## Modes

Spanning tree MSTP configuration mode

## Usage Guidelines

The following rules apply:

- VLANs must be created before mapping to instances.
- The VLAN instance mapping is removed from the configuration if the underlying VLANs are deleted.

Enter **no instance** to remove the VLAN mapping from the MSTP instance.



### CAUTION

This command can be used only after the VLAN is defined.

## Examples

To map a VLAN to an MTSP instance:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# instance 1 vlan 2,3
device(conf-mstp)# instance 2 vlan 4-6
device(conf-mstp)# instance 1 priority 4096
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# interface management

Accesses management interface configuration mode for the specified management interface.

## Syntax

```
interface management { 1 | 2 }
```

## Parameters

- 1  
Accesses the configuration mode for management interface 1.
- 2  
Accesses the configuration mode for management interface 2.

## Modes

Global configuration mode

## Usage Guidelines

The mode allows you to configure the parameters of the specified management interface.

## Examples

The following example accesses the interface management mode for management interface 1.

```
device# configure terminal
device(config)# interface Management 1
device(config-Management-1)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# interval

For an implementation of an event-handler profile, specifies the number of seconds between iterations of an event-handler action, if triggered.

## Syntax

`interval seconds`

`no interval`

## Command Default

Iterations occur with no interval between them.

## Parameters

*seconds*

Specifies the number of seconds between iterations of an event-handler action, if triggered. Valid values are 0 or a positive integer.

## Modes

Event-handler activation mode

## Usage Guidelines

The **interval** command is effective only if the **iterations** value is non-zero.

The **no** form of this command resets the **interval** setting to the default 0 seconds.

## Examples

The following example sets the number of iterations to 3 and specifies an interval of 10 seconds between each iteration.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# iterations 3
device(config-activate-eventHandler1)# interval 10
```

The following example resets **interval** to the default value of 0 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no interval
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip access-group

Applies rules specified in an IPv4 access control list (ACL) to traffic entering or exiting an interface.

## Syntax

```
ip access-group ACLname { in | out }
```

```
no ip access-group ACLname { in | out }
```

## Parameters

*ACLname*

Specifies the name of the standard or extended IPv4 access list.

**in**

Applies the ACL to incoming switched and routed traffic.

**out**

Applies the ACL to outgoing routed traffic.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to apply an IPv4 ACL to one of the following interface types:

- User interfaces
  - Physical Ethernet interfaces
  - Logical interfaces (LAGs)
  - Virtual Ethernet interfaces (VEs)
- All supported management interfaces

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of two ACLs to a management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces. And you can apply an ACL twice—ingress and egress—to a given user interface.

To remove an ACL from an interface, enter the **no** form of this command.

## Examples

The following example applies an ingress IP ACL on an Ethernet interface:

```
device(config)# interface ethernet 2/2
device(conf-if-eth-2/9)# ip access-group ipacl2 in
```

The following example removes an ingress IP ACL from an Ethernet interface:

```
device(config)# interface ethernet 2/2
device(conf-if-eth-2/9)# no ip access-group ipacl2 in
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ip access-list

Creates a standard or extended IPv4 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

## Syntax

```
ip access-list { standard | extended } ACLname
no ip access-list { standard | extended } ACLname
```

## Parameters

### standard | extended

Specifies one of the following types of access lists:

#### standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

#### extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

### *ACLname*

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

## Modes

Global configuration mode

## Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a-z, A-Z or 0-9. You can also use underscore (\_) or hyphen (-) in an ACL name, but not as the first character.

On any given device, an ACL name must be unique among all ACL types (MAC/IPv4/IPv6; standard or extended).

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after it is applied to an interface, using the **access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

## Examples

The following example creates an IPv4 standard ACL.

```
device# configure
device(config)# ip access-list standard stdACL3
```

The following example creates an IPv4 extended ACL.

```
device# configure
device(config)# ip access-list extended extdACL5
```

The following example creates rules on an IPv4 standard ACL.

```
device# configure
device(config)# ip access-list standard stdACL3
device(config-ipacl-std)# seq 5 permit host 10.20.33.4
device(config-ipacl-std)# seq 15 deny any
```

The following example deletes an IPv4 ACL.

```
device# configure
device(config)# no ip access-list standard stdACL3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip address

Configures an IP address on an interface.

## Syntax

```
ip address ip-address/mask ospf-ignore ]]
```

```
no ip address [ ip-address/mask ]
```

## Parameters

*ip-address*

Specifies the IP address.

*mask*

Specifies the mask for the associated IP subnet. Dotted-decimal notation is not supported. For non-loopback interfaces, valid values are from 1 through 31. For loopback interfaces, the only valid value is 32.

**ospf-ignore**

Disables adjacency formation with OSPF neighbors and disables advertisement of the interface to OSPF.

**ospf-passive**

Disables adjacency formation with OSPF neighbors but does not disable advertisement of the interface to OSPF.

## Modes

Interface configuration mode

Management interface configuration mode

## Usage Guidelines

- Use this command to configure a primary or secondary IP address for a specific interface. You can also use this command to prevent OSPF from running on specified subnets. Multiple primary IP addresses are supported on an interface.
- You can use this command to configure a primary or secondary IP address for a management interface.
- For a management interface, only one primary IP address is supported. Secondary IP addresses are not supported.
- A primary IP address cannot overlap with a previously configured IP subnet.
- A primary IP address must be configured before you configure a secondary IP address in the same subnet.
- To remove the configured static or DHCP address, enter **no ip address**. This resets the address to 0.0.0.0/0.
- The **no** form of the command removes a specific IP address from the interface.

## Examples

The following example configures a primary IP address on a specified Ethernet interface.

```
device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# ip address 10.1.1.1/24
```

The following example replaces the primary IP address of an interface .

```
device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# ip address 10.1.1.2/24 secondary
```

The following example configures a primary IP address on a management interface.

```
device(config)# interface Management 1/0
device(config-Management-1/0)# no ip address
device(config-Management-1/0)# ip address 10.1.1.2/24
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip arp-aging-timeout

Sets how long a dynamic Address Resolution Protocol (ARP) entry stays in the ARP cache. The aging timer is reset each time an ARP reply is received.

## Syntax

```
ip arp-aging-timeout value
```

```
no ip arp-aging-timeout
```

## Command Default

ARP aging timeout is globally enabled and set to 240 minutes.

## Parameters

*value*

Specifies how long an ARP entry stays in the ARP cache. Values range from 0 through 240 minutes.

## Modes

Interface subtype configuration mode

## Usage Guidelines

When the device places an entry in the ARP cache, the device also starts an aging timer for the entry. The aging timer ensures that the ARP cache does not retain learned entries that are no longer valid. An entry can become invalid when the device with the MAC address of the entry is no longer on the network.

The aging timer is reset each time an ARP reply is received.

Aging out affects dynamic (learned) entries only. Static entries do not age out.

You can modify the ARP aging timeout only at the interface level, but not at the global level.

To prevent entries from aging out, enter **ip arp-aging-timeout 0**.

The **no** form of the command restores the default aging timeout of 240 minutes.

## Examples

The following command sets the ARP aging timeout to 100 minutes on an interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# ip arp-aging-timeout 100
```

The following command restores the ARP aging timeout to the default value of 240 minutes on an interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# no ip arp-aging-timeout
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip dhcp relay address

Configures the IP DHCP Relay on a Layer 3 interface.

## Syntax

```
ip dhcp relay address ip-addr [ use-vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

**use-vrf**

Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

*vrf-name*

VRF name.

## Modes

Interface configuration mode

## Usage Guidelines

This command uses the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

Enter the command while in interface configuration mode for a VE or Ethernet interface where you want to configure the IP DHCP Relay. Configure up to sixteen DHCP server IP addresses per interface.

Use the **no** version of this command to remove the IP DHCP relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

## Examples

To configure an IP DHCP Relay address on a Ve interface:

```
device# config
device(config)# interface ve 100
device(config-Ve-100)# ip dhcp relay address 3.1.2.255 use-vrf blue
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip dhcp relay gateway address

Configures the IP DHCP Relay on a Layer 3 gateway interface.

## Syntax

```
ip dhcp relay gateway address ip-addr
no ip dhcp relay gateway address ip-addr
```

## Parameters

*ip-addr*

IPv4 gateway address of the DHCP server where the DHCP client requests are to be forwarded.

## Modes

Interface configuration mode

## Usage Guidelines

Use this command to configure the IP DHCP Relay on the switch Layer 3 gateway interface using the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

Use the **no** version of this command to remove the IP DHCP Relay from the interface.

## Examples

To configure an IP DHCP Relay address on an interface:

```
device(config)# interface ethernet 1/4
device(config-if-eth-1/4)# ip dhcp relay gateway 10.50.22.26
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ip dns

Configures the Domain Name System (DNS) domain name and the primary and secondary name server IP addresses.

## Syntax

```
ip dns { domain-name domain-name | name-server ip-address-of-name-server }
no ip dns { domain-name domain-name | name-server ip_address_of_name_server }
```

## Parameters

**domain-name** *domain-name*

Specifies the DNS domain name.

**name-server** *ip-address-of-name-server*

Specifies the IP address of the name server. IPv6 and IPv4 addresses are supported.

## Modes

Global configuration mode

## Usage Guidelines

- Your first run of **ip dns name-server** specifies the default IP gateway address. Your second run of **ip dns name-server** specifies the secondary IP gateway address.
- Name servers can only be entered or removed one at a time. The newly entered name server will append to the existing name server.
- The **no** form of the command with the domain-name parameter disables IP directed broadcasts for a specific domain.
- The **no** form of the command with the name-server parameter deletes a name server definition.

## Examples

The following example configures the DNS domain name and the primary name server IP address.

```
device(config)# ip dns domain-name mycompany.com
device(config)# ip dns name-server 10.70.20.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip icmp rate-limiting

Limits the rate at which IPv4 Internet Control Message Protocol (ICMP) messages are sent on a network.

## Syntax

```
ip icmp rate-limiting milliseconds
```

```
no ip icmp rate-limiting
```

## Command Default

This command is enabled on the management port, but is disabled on the front-end ports.

## Parameters

*milliseconds*

Time interval per ICMP packet in milliseconds. The range is from 0 through 4294967295. The default is 1000.

## Modes

Interface configuration mode

## Usage Guidelines

This is an interface-specific configuration.

The **no** form of the command will revert to the default setting. Set the interval to 0 to disable IPv4 ICMP rate-limiting.

## Examples

The following example enables IPv4 ICMP rate-limiting on an Ethernet interface.

```
device(config)# interface ethernet 3/5
device(conf-int-eth-3/5)# ip icmp rate-limiting 10000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip icmp redirect

Enables IPv4 Internet Control Message Protocol (ICMP) Redirect messages, which request that packets be sent on an alternative route.

## Syntax

```
ip icmp redirect
no ip icmp redirect
```

## Command Default

This command is enabled on both the management port and on the front-end ports.

## Modes

Interface configuration mode

## Usage Guidelines

This is an interface-specific configuration.

The **no** form of the command disables IPv4 ICMP Redirect messages.

## Examples

The following example enables IPv4 ICMP Redirect messages on an Ethernet interface.

```
device(config)# interface ethernet 2/5
device(conf-int-eth-2/5)# ip icmp redirect
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp immediate-leave

Removes a group from the IGMP table immediately following receipt of a Leave Group request.

## Syntax

```
ip igmp immediate-leave
```

```
no ip igmp immediate-leave
```

## Command Default

This command is disabled.

## Modes

Interface subtype configuration mode

## Usage Guidelines

This command treats an interface as if it had one multicast client, so that the receipt of a Leave Group request on the interface causes the group to be removed immediately from the multicast database.

Enter the **no** form of this command to restore the default behavior.

## Examples

To configure an Ethernet interface to remove a group from the IGMP table immediately following receipt of a Leave Group request:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp immediate-leave
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp last-member-query-interval

Sets the IGMP last-member query interval for an interface.

## Syntax

`ip igmp last-member-query-interval milliseconds`

`no ip igmp last-member-query-interval`

## Command Default

See Parameters.

## Parameters

*milliseconds*

Response time in milliseconds. Range is from 100 through 25500 milliseconds. The default is 1000.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The last-member query interval is the time in seconds that the IGMP router waits to receive a response to a group-specific query message, including messages sent in response to a host-leave message.

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

## Examples

To set the last-member query interval to 1500 milliseconds on an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp last-member-query-interval 1500
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp query-interval

Sets the IGMP query interval for an interface.

## Syntax

```
ip igmp query-interval seconds
```

```
no ip igmp query-interval seconds
```

## Command Default

See Parameters.

## Parameters

*seconds*

Response time in seconds. Range is from 1 through 18000 seconds. The default is 125.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The query interval is the amount of time between IGMP query messages sent by the device.

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

## Examples

To set the query interval to 500 seconds on an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp query-interval 500
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp query-max-response-time

Sets the maximum response time for IGMP queries for an interface.

## Syntax

```
ip igmp query-max-response-time seconds
```

```
no ip igmp query-max-response-time
```

## Command Default

See Parameters.

## Parameters

*seconds*

Response time in seconds. Range is from 1 through 25 seconds. The default is 10.

## Modes

Interface subtype configuration mode

## Usage Guidelines

When a host receives the query packet, it starts counting to a random value, less than the maximum response time. When this timer expires, the switch (host) replies with a report, provided that no other host from the same group has responded yet.

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

## Examples

To set the maximum response time to 20 seconds:

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp query-max-response-time 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp router-alert-check-disable

Disables the snooping check for the presence of the router alert option.

## Syntax

```
ip igmp router-alert-check-disable  
no ip igmp router-alert-check-disable
```

## Modes

Global configuration mode

## Usage Guidelines

By default, IGMP snooping checks for the presence of the router alert option in the IP packet header of the IGMP message. Packets that do not include this option are dropped.

## Examples

The following example disables the snooping router alert check globally.

```
device(config)# ip igmp router-alert-check-disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ip igmp snooping enable

Enables Internet Group Management Protocol (IGMP) snooping.

## Syntax

`ip igmp snooping enable`

`no ip igmp snooping enable`

## Modes

VLAN configuration mode

## Usage Guidelines

IGMP snooping allows a network device to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Enter `no ip igmp snooping enable` to disable snooping for a specific VLAN.

## Examples

To enable IGMP on a VLAN:

```
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping enable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp snooping fast-leave

Enables Internet Group Management Protocol (IGMP) snooping fast-leave processing for a VLAN. This allows the removal of an interface from the forwarding table without sending out group-specific queries to the interface.

## Syntax

```
ip igmp snooping fast-leave  
no ip igmp snooping fast-leave
```

## Command Default

This command is disabled.

## Modes

VLAN configuration mode.

## Usage Guidelines

Enter **no ip igmp snooping fast-leave** to disable this function.

## Examples

To enable snooping fast-leave for a specific VLAN:

```
device(config)# vlan 1  
device(config-vlan-1)# ip igmp snooping fast-leave
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp snooping last-member-query-interval

Sets the IGMP snooping last member query interval value in milliseconds.

## Syntax

```
ip igmp snooping last-member-query-interval value
no ip igmp snooping last-member-query-interval value
```

## Command Default

The default is 1000 ms.

## Parameters

*value*

Sets the value in milliseconds. The range is 100 to 25500 milliseconds.

## Modes

VLAN configuration mode

## Usage Guidelines

When a leave is received, a group-specific query is sent. Last member query interval configuration controls the time interval between last member queries sent.

## Examples

The following example sets the IGMP snooping last member query interval.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping last-member-query-interval 2000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp snooping mrouter interface

Configures a VLAN port member to be a multicast router interface.

## Syntax

```
ip igmp snooping mrouter interface { ethernet slot/port | port-channel interface number }
no ip igmp snooping mrouter interface { ethernet slot/port | port-channel interface number }
```

## Parameters

**ethernet***slot/port*

Specifies a valid port number.

**port-channel** *number*

Specifies the interface is a port-channel. Valid values range from 1 through 6144.

## Modes

VLAN configuration mode

## Usage Guidelines

A multicast router interface faces toward a multicast router or other Internet Group Management Protocol (IGMP) querier.

The **no** form of this command removes the configured mrouter.

## Examples

The following example configures a VLAN port member to be a multicast router interface.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping mrouter interface ethernet 1/1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp snooping querier enable

Activates or deactivates the Internet Group Management Protocol (IGMP) snooping querier on a VLAN.

## Syntax

```
ip igmp snooping querier enable
no ip igmp snooping querier enable
```

## Command Default

IGMP snooping querier is disabled.

## Modes

VLAN configuration mode

## Usage Guidelines

Enter **no ip igmp snooping querier enable** to disable the IGMP snooping querier.

## Examples

To enable the IGMP snooping querier on the VLAN:

```
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping querier enable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp snooping query-interval

Sets the IGMP snooping query interval in seconds.

## Syntax

`ip igmp snooping query-interval seconds`

`no ip igmp snooping query-interval seconds`

## Command Default

The default is 125 seconds.

## Parameters

*seconds*

Sets the IGMP snooping query interval in seconds. The range is 1-18000 seconds.

## Modes

VLAN configuration mode

## Usage Guidelines

The `ip igmp snooping query-interval` command allows you to modify the query interval, which specifies how often the SLX-OS device enabled for active IGMP snooping sends group membership queries.

## Examples

The following example sets the IGMP snooping query interval.

```
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping query-interval 200
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp snooping query-max-response-time

Sets the IGMP snooping query maximum response time.

## Syntax

```
ip igmp snooping query-max-response-time seconds
```

```
no ip igmp snooping query-max-response-time seconds
```

## Command Default

The default is 10 seconds.

## Parameters

*seconds*

Specifies the IGMP snooping query maximum response time in seconds. The range is 1 to 25 seconds.

## Modes

VLAN configuration mode

## Usage Guidelines

The IGMP snooping query maximum response time is the length of time in seconds that the device will wait for an IGMP (V1 or V2) response from an interface before concluding that the group member on that interface is down and removing it from the group.

## Examples

The following example sets the IGMP snooping query max response time.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping query-max-response-time 15
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp snooping static-group

Configures an interface in a VLAN as a static member of a multicast group.

## Syntax

```
ip igmp snooping static-group { ip-address } {interface ethernet/port-channel }
```

```
ip igmp snooping static-group { ip-address } {interface ethernet/port-channel }
```

## Parameters

*ip-address*

Specifies the multicast address to be joined in the A.B.C.D format.

**interface**

Specifies the interface.

*ethernet/port-channel*

Specifies the interface type.

## Modes

VLAN configuration mode

## Usage Guidelines

A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports. If clients cannot send reports, you can configure a static group which applies to specific ports. The static group allows packets to be forwarded to the static group ports even though they have no client membership reports.

## Examples

The following example sets the IGMP snooping static-group.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ip igmp snooping static-group 225.0.0.1 interface ethernet 6/15
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ip igmp ssm-map

Enables the IGMPv2 Source Specific Multicast mapping.

## Syntax

```
ip igmp ssm-map [ ASCII string | enable source-address ]
no ip igmp ssm-map [ ASCII string | enable source-address ]
```

## Parameters

*ASCII string*

Specifies the prefix list name.

**enable***source-address*

Specifies the source address.

## Modes

Global configuration mode

Router PIM configuration mode

## Usage Guidelines

A prefix list is used for SSM mapping with permit clauses.

Use the **no** form of this command to disable SSM mapping.

## Examples

The following example enables the SSM mapping for IGMPv2 and configures an SSM map at the global level.

```
device(config)# ip igmp ssm-map enable
device(config)# ip igmp ssm-map ssm-map-230-to-232 203.0.0.10
device(config)# ip igmp ssm-map ssm-map-233-to-234 204.0.0.10
```

The following example enables the SSM range configuration at the router PIM level.

```
device(config)# router pim
  device(config-pim-router)# ssm-enable range PL_ssm_range -230-to-234
```

The following example shows a prefix list configuration for the SSM range.

```
device(config)# ip prefix-list PL_ssm_range seq 5 permit 230.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 231.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 232.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 233.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 234.0.0.0/8
```

The following example shows a prefix list configuration for an SSM map.

```
device(config)# ip prefix-list ssm-map-230-to-232 seq 5 permit 230.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 10 permit 231.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 15 permit 232.0.0.0/8

device(config)# ip prefix-list ssm-map-233-to-234 seq 5 permit 233.0.0.0/8
device(config)# ip prefix-list ssm-map-233-to-234 seq 10 permit 234.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 15 permit 232.0.0.0/8
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp static-group

Configures the IGMP static group membership entries for a specific interface.

## Syntax

```
ip igmp static-group A.B.C.D
no ip igmp static-group A.B.C.D
```

## Parameters

*A.B.C.D*

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses to be included in the multicast group.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **ip igmp static-group** command creates IGMP static group membership to test multicast forwarding without a receiver host. Traffic is forwarded to an interface without the need to receive membership reports from host members. Packets to the group are fast-switched out of a specific interface. Static group membership entries are automatically added to the IGMP cache and the PIM mcache table.

## Examples

To create a static multicast group for an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp static-group 225.0.0.10 interface ethernet 6/15
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip igmp version

Specifies the IGMP version on a device.

## Syntax

```
ip igmp version version-number
no ip igmp version version-number
```

## Command Default

IGMP Version 2 is enabled.

## Parameters

*version-number*  
Specifies the version number: 1, 2, or 3. Version 2 is the default.

## Modes

Interface configuration mode

## Usage Guidelines

The **no** form of this command restores the default; IGMP Version 2 is enabled.

## Examples

The following example, in interface configuration mode, enables IGMP Version 3 for a physical port.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(config-if-1/5)# ip igmp version 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip mtu

Sets the IP maximum transmission unit (MTU) on a specified interface.

## Syntax

`ip mtu size`

`no ip mtu`

## Command Default

The default IP MTU size is 1500 bytes.

## Parameters

*size*

Specifies the size of an interface IP MTU. Values range from 1300 through 9194 bytes.

## Modes

Interface configuration mode

## Usage Guidelines

If the interface is part of a VE, change the IPv4 MTU only at the VE interface and not at the physical port. All member ports of a VE inherit the VE-interface IPv4 MTU value.

The **no** form of the command reverts the MTU size to the default value.

## Examples

The following example sets the IP MTU to 2000 bytes on the specified Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/9
device(config-if-eth-2/9)# ip mtu 2000
```

The following example changes the IP MTU for a VE.

```
device(config)# interface ve 103
device(config-vif-103)# ip mtu 2000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf active

Sets a specific OSPF interface to active.

## Syntax

```
ip ospf active
```

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use the **ip ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPF control packets.

## Examples

The following example sets a specific OSPFv2 Ethernet interface to active.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf active
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf area

Enables OSPFv2 on an interface.

## Syntax

```
ip ospf area area-id | ip-addr
no ip ospf area
```

## Command Default

Disabled.

## Parameters

*area-id*  
Area ID in decimal format. Valid values range from 1 through 2147483647.

*ip-addr*  
Area ID in IP address format.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **no** form of the command disables OSPFv2 on the interface.

## Examples

The following example enables a configured OSPFv2 area named 1 on a specific OSPFv2 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf area 1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf auth-change-wait-time

Configures authentication-change hold time.

## Syntax

```
ip ospf auth-change-wait-time wait-time  
no ip ospf auth-change-wait-time
```

## Command Default

Wait time is 300 seconds

## Parameters

*wait-time*

Time before an authentication change takes place. Valid values range from 0 to 14400 seconds.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to set or reset the authentication change hold time for the interface to which you are connected.

OSPFv2 provides graceful authentication change for the following types of authentication changes:

Changing authentication methods from one of the following to another of the following:

- Simple text password
- MD5 authentication
- No authentication

Configuring a new simple text password or MD5 authentication key.

Changing an existing simple text password or MD5 authentication key

The **no** form of the command resets the wait time to the default of 300 seconds.

## Examples

The following example sets the wait time to 400 seconds on a specific OSPF virtual Ethernet (VE) interface.

```
device# configure terminal  
device(config)# interface ve 1  
device(config-if-Ve-1)# ip ospf auth-change-wait-time 400
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf authentication-key

Configures simple password-based authentication for OSPF.

## Syntax

```
ip ospf authentication-key password
no ip ospf authentication-key
```

## Command Default

Authentication is disabled.

## Parameters

*password*  
OSPF processes *password* as a plain text password.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to set or reset simple password-based authentication on the OSPFv2 interface to which you are connected. The **no** form of the command disables OSPFv2 authentication.

## Examples

The following example configures an authentication key for an OSPF virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf authentication-key morningadmin
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf cost

Configures cost for a specific interface.

## Syntax

```
ip ospf cost value
no ip ospf cost
```

## Command Default

Cost value is 1.

## Parameters

*value*

Cost value. Valid values range from 1 through 65535. The default is 1.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to set or reset the OSPFv2 cost on the interface. If the cost is not configured with this command, OSPFv2 calculates the value from the reference and interface bandwidths.

The **no** form of the command disables the configured cost.

## Examples

The following example sets the cost to 520 on a specific Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ip ospf cost 520
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf database-filter

Configures filters for different types of outgoing Link State Advertisements (LSAs).

## Syntax

```
ip ospf database-filter { all-external | all-summary-external { allow-default-and-type-4 | allow-default-out | out } }
```

```
ip ospf database-filter all-out
```

```
no ip ospf database-filter all-external
```

```
no ip ospf database-filter all-out
```

```
no ip ospf database-filter all-summary-external
```

## Command Default

All filters are disabled.

## Parameters

### all-external

Blocks all external LSAs.

### all-summary-external

Blocks all summary (Type 3) and external (type 5) LSAs.

### allow-default-and-type-4

Allows default-route LSAs and Type 4 LSAs, but block all other LSAs.

### allow-default-out

Allows default-route LSAs, but block all other LSAs.

### out

Filters outgoing LSAs.

### all-out

Blocks all LSAs.

## Modes

Interface subtype configuration mode

## Usage Guidelines

By default, the device floods all outbound LSAs on all the OSPF interfaces within an area. You can configure a filter to block outbound LSAs on an OSPF interface. This feature is particularly useful when you want to block LSAs from some, but not all, of the interfaces attached to the area. When enabled, this command blocks the specified outgoing LSAs on the interface. Some cases where you might want to enable filters are:

- To control the information being advertised to the network.
- To use a passive router for debugging only.

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

**NOTE**

You cannot block LSAs on virtual links.

## Examples

The following example applies a filter to block flooding of all LSAs on a specific OSPF Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# ip ospf database-filter all-out
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf dead-interval

Configures the neighbor dead interval, which is the number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down.

## Syntax

```
ip ospf dead-interval interval
```

```
no ip ospf dead-interval
```

## Command Default

The specified time period is 40 seconds.

## Parameters

*interval*

Dead interval in seconds. Valid values range from 3 through 65535 seconds. The default is 40.

## Modes

Interface subtype configuration mode

## Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the **ip ospf hello-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is  $\frac{1}{4}$  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 200 on a specific OSPFv2 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf dead-interval 200
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf hello-interval

Configures the hello interval, which is the length of time between the transmission of hello packets that this interface sends to neighbor routers.

## Syntax

```
ip ospf hello-interval interval
```

```
no ip ospf hello-interval
```

## 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  $\frac{1}{4}$  times that of the dead interval.

The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello-interval change is not displayed.

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

## Examples

The following example sets the hello interval to 50 on a specific OSPFv2 virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf hello-interval 50
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf ldp-sync

Enables Label Distribution Protocol (LDP) synchronization with OSPF and configures the hold down time interval for an interface.

## Syntax

```
ip ospf ldp-sync { disable | enable }
no ip ospf ldp-sync enable
```

## Command Default

Disabled.

## Parameters

**disable**  
Disables LDP synchronization.

**enable**  
Enables LDP synchronization.

## Modes

Interface subtype configuration mode

## Examples

The following example enables LDP synchronization with OSPF for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# ip ospf ldp-sync enable
```

The following example disables LDP synchronization with OSPF for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-loopback-1)# ip ospf ldp-sync disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf md5-authentication

Configures MD5 password and authentication change hold time.

## Syntax

```
ip ospf md5-authentication { key-activation-wait-time wait-time | key-id id key password }  
no ip ospf md5-authentication key-id
```

## Command Default

No authentication.

## Parameters

### **key-activation-wait-time** *wait-time*

Sets the time that OSPFv2 waits before activating a new MD5 key. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends use the newly configured MD5 Key. OSPFv2 packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. Valid values range from 0 to 14400 seconds.

### **key-id**

Sets MD5 key.

*id*

Identifies the MD5 key ID. Valid values range from 1 and 255.

### **key password**

Specifies the MD5 authentication ID and sets a password.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to set or reset the MD5 password and/or authentication change hold time on the interface to which you are connected.

By default, the authentication key is encrypted. If you want the authentication key to be in clear text, insert a O between authentication-key and string. The software adds a prefix to the authentication key string in the configuration. For example, the following portion of the code has the encrypted code "2".

Enter **no ip ospf md5-authentication key-id** to disable this configuration.

## Examples

The following example sets the time that OSPFv2 waits before activating a new MD5 key to 240 seconds on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf md5-authentication key-activation-wait-time 240
```

The following example sets the MD5 key ID to 22 and a password "myospfpassword" on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf md5-authentication key-id 22 key myospfpassword
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

## Syntax

```
ip ospf mtu-ignore
no ip ospf mtu-ignore
```

## Command Default

Enabled

## Modes

Interface subtype configuration mode

## Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv2 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The **no** form of the command disables MTU-match checking on a specific interface.

## Examples

The following example disables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no ip ospf mtu-ignore
```

The following example enables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf mtu-ignore
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf network

Configures the network type for the interface. Point-to-point can support unnumbered links, which requires less processing by OSPF.

## Syntax

```
ip ospf network { broadcast | non-broadcast | point-to-point }  
no ip ospf network
```

## Command Default

Network type is broadcast.

## Parameters

### broadcast

Network type is broadcast.

### non-broadcast

Network type is non-broadcast. An interface can be configured to send OSPF traffic to its neighbor as unicast packets rather than multicast packets.

### point-to-point

Network type is point-to-point.

## Modes

Interface subtype configuration mode

## Usage Guidelines

On a non-broadcast interface, the devices at either end of the interface must configure non-broadcast interface type and the neighbor IP address. There is no restriction on the number of devices sharing a non-broadcast interface.

To configure an OSPF interface as a non-broadcast interface, the feature must be enabled on a physical interface or a VE, following the **ip ospf area** statement, and then specify the IP address of the neighbor in the OSPF configuration. The non-broadcast interface configuration must be done on the OSPF devices at either end of the link.

The **no** form of the command removes the network-type configuration.

## Examples

The following example configures an OSPFv2 point-to-point link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal  
device(config)# interface ethernet 1/1  
device(conf-if-eth-1/1)# ip ospf network point-to-point
```

The following example configures an OSPFv2 broadcast link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf network broadcast
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# 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

Passive interfaces accept and process all OSPF protocol traffic, but they do not send any traffic.

You might want to set an interface to passive mode if:

- You are planning to use the router mostly for debugging purposes.
- The router is a stub and does not route traffic.

The **no** form of the command sets an interface back to active.

## Examples

The following example sets a specific OSPFv2 Ethernet interface to passive.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf passive
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ip ospf priority

Configures priority for designated router (DR) election.

## Syntax

```
ip ospf priority value
no ip ospf priority
```

## Command Default

The default value is 1.

## Parameters

*value*  
Priority value. Valid values range from 0 through 255.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The OSPFv2 router assigned the highest priority becomes the designated router, and the OSPFv2 router with the second-highest priority becomes the backup router.

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

## Examples

The following example sets a priority of 10 for the OSPFv2 router that is connected to an OSPFv2 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf priority 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

## Syntax

```
ip ospf retransmit-interval interval
no ip ospf retransmit-interval
```

## Command Default

The interval is 5 seconds.

## Parameters

*interval*

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

## Examples

The following example sets the retransmit interval to 8 for all OSPFv2 devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf retransmit-interval 8
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv2 to send link-state update packets on the interface to which you are connected.

## Syntax

```
ip ospf transmit-delay value
```

```
no ip ospf transmit-delay
```

## Command Default

The transmit delay is set to 1 second.

## Parameters

*value*

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

## Modes

Interface subtype configuration mode

## Usage Guidelines

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

## Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf transmit-delay 25
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip pim dr-priority

Configures the designated router (DR) priority on IPv4 interfaces.

## Syntax

```
ip pim dr-priority priority-value  
no ip pim dr-priority priority-value
```

## Command Default

The default DR priority value is 1.

## Parameters

*priority-value*  
Specifies the DR priority value as an integer. The range is 0 through 65535.

## Modes

Interface configuration mode

## Usage Guidelines

The **no** form of this command restores the default DR priority value, 1.

You must enable PIM globally before you enable it on an interface.

You can configure the **ip pim dr-priority** command in either Dense mode (DM) or Sparse mode (SM).

If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IP address on that subnet is elected as the DR.

The DR priority information is used in the DR election only if all the PIM devices connected to the subnet support the DR priority option. If at least one PIM device on the subnet does not support this option, the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IP address on the subnet is declared the DR regardless of the DR priority values.

## Examples

This example configures a DR priority value of 50.

```
device(config)# interface ethernet 1/1  
device(config-if-e10000-1/1)# ip pim dr-priority 50
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip pim-sparse

Enables or disables Protocol Independent Multicast Sparse Mode on port channels, physical or VE interfaces.

## Syntax

```
ip pim-sparse
no ip pim-sparse
```

## Command Default

Protocol Independent Multicast (PIM) is not enabled on an interface.

## Modes

Interface subtype configuration mode

## Usage Guidelines

PIM must be enabled on the device before enabling PIM-sparse. PIM-sparse can be enabled on interfaces

Enter **no ip pim-sparse** to disable this feature.

## Examples

To enable PIM Sparse Mode on a virtual Ethernet (VE) interface:

```
device(config)# int ve 1
device(config-if-Ve-1)# ip pim-sparse
```

To enable PIM Sparse Mode on a router port:

```
device(config)# int eth 1/1
device(config-if-eth-1/1)# ip pim-sparse
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip pim ttl-threshold

Sets the IP PIM time to live (TTL) threshold.

## Syntax

```
ip pim ttl-threshold value
```

```
ip pim ttl-threshold
```

## Command Default

The default value is 1.

## Parameters

*priority value*

Specifies the TTL threshold value. The range is 1 to 64.

## Modes

Interface configuration mode

## Usage Guidelines

The TTL threshold defines the minimum value required in a packet for it to be forwarded out of the interface after the TTL has been decremented.

For example, if the TTL for an interface is set at 10, only those packets that enter with a TTL value of 11 or more are forwarded through the TTL-10 interface. With a default TTL threshold of 1, only packets ingressing with a TTL of 2 or greater are forwarded. The TTL threshold only applies to routed interfaces and is ignored by switched interfaces. Possible TTL values are 1 to 64. The default TTL value is 1.

The **no** form of the command restores the default TTL threshold 1.

## Examples

The following example sets the TTL value.

```
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip pim ttl-threshold 50
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip policy route-map

Enables policy-based routing (PBR).

## Syntax

```
ip policy route-map map-name
```

```
no ip policy route-map map-name
```

## Command Default

PBR is not enabled.

## Parameters

*map-name*

Specifies the name of the route map.

## Modes

Interface configuration mode

Virtual interface configuration mode

## Usage Guidelines

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

## Examples

The following example enables PBR on a specific interface.

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# match ip address acl 99
device(config-route-map-test-route/permit/99)# set ip next-hop 192.168.3.1
device(config-route-map-test-route/permit/99)# exit
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip policy route-map test-route
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ip proxy-arp

Enables Proxy Address Resolution Protocol (APR) on an interface.

## Syntax

```
ip proxy-arp
no ip proxy-arp
```

## Command Default

Proxy ARP is enabled.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Proxy ARP enables a device to answer ARP requests from devices in one network on behalf of devices in another network. Because ARP requests are MAC-layer broadcasts, they reach only the devices that are directly connected to the sender of the ARP request. Therefore, ARP requests do not cross routers.

The **no** form of the command disables Proxy ARP on an interface.

## Examples

The following example disables Proxy ARP on a specified interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# no ip proxy-arp
```

The following example enables Proxy ARP on a specified interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# ip proxy-arp
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip receive access-group

Applies an IPv4 access control list (ACL) at global configuration level. Such *receive-path* ACLs filter incoming route-processor traffic according to rules that you create.

## Syntax

```
ip receive access-group acl-name  
no ip receive access-group acl-name
```

## Command Default

No receive-path ACLs are applied.

## Parameters

*acl-name*  
Specifies the name of the standard or extended IP access list.

## Modes

Global configuration mode

## Usage Guidelines

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny/hard-drop rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL, from an interface-subtype configuration mode you use the { **ip | ipv6 | mac** } **access-group** command.
- To apply a receive-path ACL, from global configuration mode you use the { **ip | ipv6** } **receive access-group** command.

You can apply a maximum of two receive-path ACLs to a device, as follows:

- One IPv4 receive-path ACL
- One IPv6 receive-path ACL

To remove a receive-path ACL, enter the **no** form of this command.

## Examples

The following example creates an IPv4 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ip access-list extended ipv4-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20.0.0.1 count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq bgp count

device(conf-ipacl-ext)# exit
device(config)# ip receive access-group ipv4-receive-acl-example
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip route

Adds a static route to the IP routing table.

## Syntax

```
ip route dest-ip-addr [ next-hop-vrf next-vrf-name ] next-hop-address [ metric ] [ distance distance ] [ tag tag-number ]
ip route dest-ip-addr { ethernet slot/port | ve ve-number } [ metric ] [ distance distance ] [ tag tag-number ]
ip route dest-ip-addr null 0 [ metric ] [ distance distance ] [ tag tag-number ]
no ip route dest-ip-addr [ next-hop-vrf next-vrf-name ] next-hop-address [ metric ] [ distance distance ] [ tag tag-number ]
no ip route dest-ip-addr { ethernet slot/port | ve ve-number } [ metric ] [ distance distance ] [ tag tag-number ]
no ip route dest-ip-addr null 0 [ metric ] [ distance distance ] [ tag tag-number ]
```

## Parameters

**next-hop-vrf** *vrf-name*

Specifies the name of the non-default VRF to be used for as the next-hop gateway.

*dest-ip-addr*

Specifies the destination IPv4 address and mask in the format A.B.C.D/L (where "L" is the prefix length of the mask).

*next-hop-addr*

Specifies the IPv4 address of the next hop.

**ethernet** *slot/port*

Specifies the destination Ethernet port.

**next-hop-vrf** *next-vrf-name*

VRF name of next hop.

**ve** *vlan-id*

Specifies the outgoing interface type as VE.

**null 0**

Configures the Layer 3 switch to drop IP packets to a specific network or host address by configuring a "null" (sometimes called "null0") static route for the address.

*metric*

Specifies the cost metric of the route. Valid values range from 1 through 16. The default is 1.

**distance** *distance*

Specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, an SLX-OS device prefers lower administrative distances over higher ones. Valid values range from 1 through 254. The default is 1.

**tag** *tag-number*

Specifies the tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295. The default is 0.

## Modes

Global configuration mode

## Usage Guidelines

The **no** form of the command followed by the route identifier removes a static route.

If you do not want to specify a next-hop IP address, you can instead specify a physical or virtual interface on the SLX-OS device. If you specify an Ethernet port, the device forwards packets destined for the static route's destination network to the specified interface. Conceptually, this feature makes the destination network like a directly connected network, associated with an SLX-OS device interface.

The port or virtual interface you use for the static route's next hop must have at least one IP address configured on it. The address does not need to be in the same subnet as the destination network.

For a default route, use the following as the destination IP address 0.0.0.0/0.

You can create a null route for traffic for traffic that should not be forwarded. To create a null route, use the key phrase **null 0** as the next hop.

## Examples

The following example configures a static route to 10.95.7.0 addresses, using 10.95.6.157 as the next-hop gateway.

```
device(config)# ip route 10.95.7.0/24 10.95.6.157
```

The following example configures a default route to next-hop IP address 10.24.4.1.

```
device(config)# ip route 0.0.0.0/0 10.24.4.1
```

The following example configures a static route with an Ethernet interface as the destination.

```
device(config)# ip route 192.128.2.69/24 ethernet 4/1
```

The following example configures a null static route to drop packets destined for network 10.157.22.x.

```
device(config)# ip route 10.157.22.0/24 null 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip router-id

Changes the router ID that is already in configured.

## Syntax

```
ip router-id A.B.C.D
no ip router-id A.B.C.D
```

## Parameters

*A.B.C.D*  
Specifies the IPv4 address that you want as the router ID.

## Modes

Global configuration mode  
VRF configuration mode

## Usage Guidelines

Though a device has IP addresses assigned to various interfaces, some routing protocols identify the device by the router ID rather than the IP addresses assigned to the interfaces connected by the protocol.

The **no** form of the command removes the configured router ID and restores the default router ID.

## Examples

The following example specifies the router ID as 192.158.1.2.

```
device# configure terminal
device(config)# ip router-id 192.158.1.2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing at the interface level.

## Syntax

```
ip router isis
```

## Command Default

Disabled.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use the **no** form of this command to disable IS-IS routing for the interface.

## Examples

The following example enables IS-IS routing for an interface Ethernet.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip router isis
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ip vrrp-extended auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol Extended (VRRP-E) interface.

## Syntax

```
ip vrrp-extended auth-type md5-auth auth-text  
no ip vrrp-extended auth-type md5-auth
```

## Command Default

No authentication is configured for a VRRP-E interface.

## Parameters

### **auth-type**

Authentication type used to verify the *password*.

### **md5-auth** *auth-text*

Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

## Modes

Virtual Ethernet (ve) interface configuration mode

## Usage Guidelines

This configuration is for virtual Ethernet (ve) interfaces only.

If the **md5-auth** option is configured, syslog and SNMP traps are generated if a packet is being dropped due to MD5 authentication failure. Using MD5 authentication implies that the software does not need to run checksum verification on the receiving device and can rely on the authentication code (message digest 5 algorithm) to verify the integrity of the VRRP-E message header.

The **no** form of this command removes the VRRP-E authentication from the interface.

## Examples

The following example configures MD5 authentication on Virtual Ethernet interface 20.

```
device(config)# protocol vrrp-extended  
device(config)# interface ve 20  
device(config-if-Ve-20)# ip vrrp-extended auth-type md5-auth lyk28d3j
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 access-group

Applies rules specified in an IPv6 access control list (ACL) to traffic entering an interface.

## Syntax

```
ipv6 access-group ACLname in  
no ipv6 access-group ACLname in
```

## Parameters

*ACLname*  
Specifies the name of the standard or extended IPv6 access list.

**in**  
Applies the ACL to incoming switched and routed traffic.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to apply an IPv6 ACL to one of the following interface types:

- User interfaces
  - Physical Ethernet interfaces
  - Logical interfaces (LAGs)
  - Virtual Ethernet interfaces (VEs)
- All supported management interfaces

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of two ACLs to a management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces.

To remove an ACL from an interface, enter the **no** form of this command.

## Examples

The following example applies a specified IPv6 ACL on a specified Ethernet interface to incoming traffic.

```
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# ipv6 access-group ipv6_acl_7 in
```

The following example removes a specified IPv6 ACL from a specified Ethernet interface.

```
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# no ipv6 access-group ipv6_acl_7 in
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 access-list

Creates a standard or extended IPv6 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

## Syntax

```
ipv6 access-list { standard | extended } ACLname
no ipv6 access-list { standard | extended } ACLname
```

## Parameters

### standard | extended

Specifies one of the following types of access lists:

#### standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

#### extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

### *ACLname*

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

## Modes

Global configuration mode

## Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a-z, A-Z or 0-9. You can also use underscore (\_) or hyphen (-) in an ACL name, but not as the first character.

On any given device, an ACL name must be unique among all ACL types (MAC/IPv4/IPv6; standard or extended).

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after it is applied to an interface, using the **access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

## Examples

The following example creates an IPv6 standard ACL:

```
device# configure
device(config)# ipv6 access-list standard stdV6ACL1
```

The following example creates an IPv6 extended ACL:

```
device# configure
device(config)# ipv6 access-list extended ipv6_acl_1
```

The following example creates rules on an IPv6 standard ACL:

```
device# configure
device(config)# ipv6 access-list standard stdV6ACL1
device(config-ipv6-std)# seq 10 permit 2001:db8:85a3:0:0:8a2e:370:7334
device(config-ipv6-std)# seq 11 deny any
```

The following example deletes an IPv6 ACL:

```
device# configure
device(config)# no ipv6 access-list standard stdV6ACL1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 address

Configure an IPv6 address for an interface.

## Syntax

```

ipv6 address pv6-prefix/prefix-length [ secondary ] [ anycast | eui-64 ]
no ipv6 address pv6-prefix/prefix-length [ secondary ] [ anycast | eui-64 ]
ipv6 address ipv6-address link-local
no ipv6 address ipv6-address link-local

```

## Parameters

### **ipv6-address**

Specifies the IPv6 address.

### *pv6-prefix*

Specifies the IPv6 prefix address in this format: X:X::X/M.

### *prefix-length*

A decimal value specifying the length of the IPv6 prefix.

### **secondary**

Specifies that the address is a secondary address. A maximum of 256 secondary addresses can be configured.

### **anycast**

Configures an address as an anycast address.

### **eui-64**

Configures the global address with an EUI-64 interface ID in the low-order 64 bits. The interface ID is automatically constructed in IEEE EUI-64 format using the interface's MAC address.

## Modes

Interface configuration mode

## Usage Guidelines

A secondary address cannot be configured on an interface unless the primary address is configured first.

The primary address cannot be deleted on an interface unless the secondary addresses are deleted first.

This command is not supported on loopback or management interfaces.

## Examples

### *History*

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 dhcp relay address

Configures the IPv6 DHCP Relay address on a Layer 3 interface.

## Syntax

**ipv6 dhcp relay address** *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name* ]

**no ipv6 dhcp relay address** *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name* ]

## Parameters

*ipv6-addr*

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

**interface**

This parameter specifies the outgoing interface, used when the relay address is a link-local or multicast address

*interface-type*

The type of interface - Ethernet or VE.

*interface-name*

The interface name or Ve ID.

**use-vrf**

Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

*vrf-name*

VRF name.

## Modes

Interface subtype configuration mode

## Usage Guidelines

This command uses the IPv6 address of the DHCP server where the DHCP client requests are to be forwarded. You can configure the address on a virtual Ethernet (VE) or an Ethernet interface. You can configure up to 16 relay destination addresses on an interface.

Enter the command while in interface subtype configuration mode for a VE or Ethernet interface where you want to configure the IPv6 DHCP Relay. Use the **no** version of this command to remove the IPv6 DHCP Relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

If the relay address is a link local address or a multicast address, an outgoing interface must be configured for IPv6 relay to function. In instances where the server address is relayed to a different VRF compared to a client connected interface VRF, in addition to the relay address, you must also specify the user-vrf, otherwise IPv6 relay may not function correctly. IPv6 route leaking is also required for IPv6 reachability.

The **no** form of the command deletes the IPv6 DHCP Relay address from the interface.



## Examples

To configure an IPv6 DHCP Relay address on a Ve interface:

```
device# config
device(config)# interface ve 100
device(config-Ve-100)# ipv6 dhcp relay address 2001::1122:AABB:CCDD:3344 use-vrf blue
```

To configure an IPv6 DHCP Relay address on an interface:

```
(config)# interface ethernet 2/3
device(conf-if-eth-2/3)# ipv6 dhcp relay address fe80::224:38ff:febb:e3c0 interface ethernet 2/5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 dns

Configures the DNS domain name and the primary and secondary name-server IPv6 addresses.

## Syntax

```
ipv6 dns { domain-name domain_name | name-server name_server }
```

```
no ipv6 dns { domain-name domain_name | name-server name_server }
```

## Parameters

**domain-name** *domain\_name*

Specifies the DNS domain name.

**name-server** *name\_server*

Specifies the IPv6 address of the primary and secondary name servers. Both the IPv6 and IPv4 addresses are supported.

## Modes

Global configuration mode

## Usage Guidelines

Your first run of **ipv6 dns name-server** specifies the default IP gateway address. Your second run of **ipv6 dns name-server** specifies the secondary IP gateway address.

Name servers can only be entered or removed one at a time. The newly entered name server will append to the existing name server.

To disable IP directed broadcasts for a specific domain, enter **no ipv6 dns domain-name *domain\_name***.

To delete a name-server definition, enter **no ipv6 dns name-server *ipv6\_address\_of\_name\_server***.

## Examples

The following example configures DNS.

```
device(config)# ipv6 dns domain-name mycompany.com
device(config)# ipv6 dns name-server 2001:db8:12d:1300:240z:d0ff:fe48:4672
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 icmpv6 rate-limiting

Limits the rate at which IPv6 Internet Control Message Protocol version 6 (ICMPv6) messages are sent on a network.

## Syntax

```
ipv6 icmpv6 rate-limiting milliseconds
```

```
no ipv6 icmpv6 rate-limiting
```

## Command Default

This command is enabled on the management port and on the front-end ports.

## Parameters

*milliseconds*

Time interval per ICMP packet. The range is from 1 through 4294967295 milliseconds. The default is 1000 milliseconds.

## Modes

Interface configuration mode

## Usage Guidelines

This is an interface-specific configuration.

The **no** form of this command reverts the rate limiting to the default settings.

Set the rate limiting to 0 to disable icmpv6 rate limiting.

## Examples

The following example enables IPv6 ICMP rate-limiting on an Ethernet interface.

```
device(config)# interface ethernet 3/5
device(conf-int-eth-3/5)# ipv6 icmpv6 rate-limiting
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 mtu

Sets the IPv6 maximum transmission unit (MTU) on a specified interface.

## Syntax

`ipv6 mtu size`

`no ipv6 mtu`

## Command Default

IPv6 MTU size is 1500 bytes.

## Parameters

*size*

Specifies the size of an interface IPv6 MTU. The range is from 1300 through 9216 bytes.

## Modes

Interface configuration mode

## Usage Guidelines

If the interface is part of a VE, change the IPv6 MTU only at the VE interface and not at the physical port. All member ports of a VE inherit the VE-interface IPv6 MTU value.

Use the **no ipv6 mtu** command to revert the IPv6 MTU size to the default value.

## Examples

On a specified Ethernet interface, the following example sets the IPv6 MTU to 2000 bytes.

```
device# configure terminal
device(config)# interface ethernet 2/9
device(conf-if-eth-2/9)# ipv6 mtu 2000
```

The following example changes the IPv6 MTU for a VE.

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf active

Sets a specific OSPFv3 interface to active.

## Syntax

```
ipv6 ospf active
```

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use the **ipv6 ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPFv3 control packets.

## Examples

The following example sets a specific OSPFv3 Ethernet interface to active.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf active
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf area

Enables OSPFv3 on an interface.

## Syntax

```
ipv6 ospf area area-id | ip-addr
no ipv6 ospf area
```

## Command Default

OSPFv3 is disabled.

## Parameters

*area-id*  
Area ID in dotted decimal or decimal format.

*ip-addr*  
Area ID in IP address format.

## Modes

Interface subtype configuration mode

## Usage Guidelines

This command enables an OSPFv3 area on the interface to which you are connected.

The **no** form of the command disables OSPFv3 on this interface.

## Examples

The following example enables a configured OSPFv3 area named 0 on a specific OSPFv3 Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf authentication ipsec

Specifies IP security (IPsec) as the authentication type for an OSPFv3 interface.

## Syntax

```
ipv6 ospf authentication ipsec key-add-remove-interval interval
```

```
no ipv6 ospf authentication ipsec key-add-remove-interval interval
```

## 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 Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
device(config-Loopback-1)# ipv6 ospf authentication ipsec
```

The following example sets the OSPFv3 authentication key add-remove interval to 480.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
device(config-Loopback-1)# ipv6 ospf authentication ipsec key-add-remove-interval 480
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf authentication ipsec disable

Disables IP security (IPsec) services on an OSPFv3 interface.

## Syntax

```
ipv6 ospf authentication ipsec disable
no ipv6 ospf authentication ipsec disable
```

## Command Default

Authentication is disabled.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to disable IPsec if it is enabled on the interface. Packets that are sent out will not be IPsec encapsulated and the received packets which are IPsec encapsulated will be dropped.

The **no** form of the command re-enables IPsec on the interface if IPsec is already configured on the interface.

## Examples

The following example disables IPsec on a specific OSPFv3 interface where IPsec is already enabled.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf authentication ipsec disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ipv6 ospf authentication spi

Specifies the security policy index (SPI) value for an OSPFv3 interface.

## Syntax

```
ipv6 ospf authentication spi spi { ah | esp null } { hmac-md5 | hmac-sha1 } key key }
no ipv6 ospf authentication spi
```

## Command Default

Disabled.

## Parameters

*spi*

SPI value. Valid values range from decimal numbers 512 through 4294967295.

**ah**

Specifies Authentication Header (ah) as the protocol to provide packet-level security.

**esp**

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

**null**

Specifies that the ESP payload is not encrypted.

**hmac-md5**

Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPFv3 interface.

**hmac-sha1**

Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPFv3 interface.

**key**

Number used in the calculation of the message digest.

*key*

The 40 hexadecimal character key.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Enter **no ipv6 ospf authentication spi *spi*** to remove the SPI value from the interface.

## Examples

The following example enables ESP and HMAC-SHA-1 on a specified OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# ipv6 ospf area 0
device(config-if-eth-1/1)# ipv6 ospf authentication spi 512 esp null hmac-sha1 key
abcef12345678901234fedcba098765432109876
```

The following example enables HA and HMAC-MD5 on a specified OSPFv3 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf area 0
device(config-if-Ve-1# ipv6 ospf authentication spi 750 ha hmac-md5 key
abcef12345678901234fedcba098765432109876
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf cost

Configures cost for a specific OSPFv3 interface.

## Syntax

```
ipv6 ospf cost value
no ipv6 ospf cost
```

## Command Default

Cost value is 1.

## Parameters

*value*

Cost value. Valid values range from 1 through 65535. The default is 1.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use this command to set or reset the OSPFv3 cost on the interface. If the cost is not configured with this command, OSPFv3 calculates the value from the reference and interface bandwidths.

For more information, refer to the **auto-cost reference-bandwidth** command.

The **no** form of the command disables the configured cost.

## Examples

The following example sets the cost to 620 on a specific OSPFv3 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf cost 620
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf dead-interval

Specifies the time period for which a neighbor router waits for a hello packet from the device before declaring the router down.

## Syntax

```
ipv6 ospf dead-interval interval
no ipv6 ospf dead-interval
```

## 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(conf-if-eth-1/1)# ipv6 ospf dead-interval 80
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf hello-interval

Sets the length of time between the transmission of hello packets that an interface sends to neighbor routers.

## Syntax

```
ipv6 ospf hello-interval interval  
no ipv6 ospf hello-interval
```

## 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  $\frac{1}{4}$  times that of the dead interval.

The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello interval change is not displayed.

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

## Examples

The following example sets the hello interval to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal  
device(config)# interface ethernet 1/1  
device(conf-if-eth-1/1)# ipv6 ospf hello-interval 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf hello-jitter

Sets the allowed jitter between HELLO packets.

## Syntax

```
ipv6 ospf hello-jitter interval
no ipv6 ospf hello-jitter
```

## Command Default

10%

## Parameters

*jitter*

Allowed interval between hello packets. Valid values range from 1 through 50 percent (%).

## Modes

Interface subtype configuration mode

## Usage Guidelines

The hello interval can vary from the configured hello-interval to a maximum of percentage value of configured jitter.

## Examples

The following example sets the hello jitter to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf hello-jitter 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf instance

Specifies the number of OSPFv3 instances running on an interface.

## Syntax

`ipv6 ospf instance instanceID`

`no ipv6 ospf instance`

## Parameters

*instanceID*

Instance identification number. Valid values range from 0 through 255.

## Modes

Interface subtype configuration mode

## Usage Guidelines

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

## Examples

The following example sets the number of IPv6 OSPF instances to 35 on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf instance 35
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ipv6 ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

## Syntax

```
ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore
```

## 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(conf-if-eth-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(conf-if-eth-1/1)# ipv6 ospf mtu-ignore
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf network

Configures network type.

## Syntax

```
ipv6 ospf network { broadcast | point-to-point }  
no ipv6 ospf network
```

## Command Default

Network type is broadcast.

## Parameters

### broadcast

Network type is broadcast, such as Ethernet.

### point-to-point

Network type is point-to-point.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Point-to-point can support unnumbered links, which requires less processing by OSPFv3.

The **no** form of the command removes the network-type configuration.

### NOTE

The network type non-broadcast is not supported at this time.

## Examples

The following example configures an OSPFv3 point-to-point link on a specific OSPFv3 Ethernet interface.

```
device# configure terminal  
device(config)# interface ethernet 1/1  
device(conf-if-eth-1/1)# ipv6 ospf network point-to-point
```

The following example configures an OSPFv3 broadcast link on a specific OSPFv3 Loopback interface.

```
device# configure terminal  
device(config)# interface loopback 1  
device(config-loopback-1)# ipv6 ospf network broadcast
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf passive

Sets a specific OSPFv3 interface to passive.

## Syntax

```
ipv6 ospf passive
no ipv6 ospf passive
```

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **ipv6 ospf passive** command disables transmission of OSPFv3 control packets on that interface. OSPFv3 control packets received on a passive interface are discarded.

The **no** form of the command sets an interface back to active.

## Examples

The following example sets a specific OSPFv3 virtual Ethernet (VE) interface to passive.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf passive
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf priority

Configures priority for designated router (DR) election and backup designated routers (BDRs) on the interface you are connected to.

## Syntax

```
ipv6 ospf priority value
```

```
no ipv6 ospf priority
```

## Command Default

The value is set to 1.

## Parameters

*value*

Priority value. Valid values range from 0 through 255. The default is 1.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The OSPFv3 router assigned the highest priority becomes the designated router, and the OSPFv3 router with the second-highest priority becomes the backup router.

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

## Examples

The following example sets a priority of 4 for the OSPFv3 router that is connected to an OSPFv3 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf priority 4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

## Syntax

```
ipv6 ospf retransmit-interval interval
no ipv6 ospf retransmit-interval
```

## Command Default

The interval is 5 seconds.

## Parameters

*interval*

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds. The default is 5.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

## Examples

The following example sets the retransmit interval to 8 for all OSPFv3 devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf retransmit-interval 8
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf suppress-linklsa

Suppresses link LSA advertisements.

## Syntax

```
ipv6 ospf suppress-linklsa
```

```
no ipv6 ospf suppress-linklsa
```

## Modes

Interface subtype configuration mode

## Examples

The following example suppresses link LSAs from being advertised on devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf suppress-linklsa
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv3 to send link-state update packets on the interface to which you are connected.

## Syntax

```
ipv6 ospf transmit-delay value
no ipv6 ospf transmit-delay
```

## Command Default

The transmit delay is set to 1 second.

## Parameters

*value*  
Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

## Modes

Interface subtype configuration mode

## Usage Guidelines

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

## Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf transmit-delay 25
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ipv6 policy route-map

Enables IPv6 policy-based routing (PBR).

## Syntax

```
ipv6 policy route-map map-name
```

```
no ipv6 policy route-map map-name
```

## Command Default

IPv6 PBR is not enabled.

## Parameters

*map-name*

Specifies the name of the route map.

## Modes

Interface configuration mode

Virtual interface configuration mode

## Usage Guidelines

The **no** form of the command disables IPv6 PBR.

## Examples

The following example enables PBR on a specific interface.

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# match ipv6 address acl 99
device(config-route-map-test-route/permit/99)# set ipv6 next-hop 2001:db8:0:0:0:ff00:42:8329
device(config-route-map-test-route/permit/99)# exit
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 policy route-map test-route
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 prefix-list

Configures an IPv6 prefix list for basic traffic filtering

## Syntax

```

ipv6 prefix-list name deny ipv6-prefix/prefix-length [ge ge-value] [le le-value]
ipv6 prefix-list name permit ipv6-prefix/prefix-length [ge ge-value] [le le-value]
ipv6 prefix-list name seq instance-number {deny ge ge-value le le-value | permit ge ge-value le le-value }
no ipv6 prefix-list name

```

## Parameters

*name*

Specifies the prefix list name.

**deny** *ip-prefix/prefix-length*

Denies a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge ge-value** or **le le-value** parameters.

**ge** *ge-value*

Specifies minimum prefix length to be matched. The range is from *ge-value* to 128.

**le** *le-value*

Specifies maximum prefix length to be matched. The range is from the *le-value* to the *prefix-length* parameter.

**permit** *ip-prefix/prefix-length*

Permits a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge ge-value** or **le le-value** parameters.

**seq**

Specifies an IPv6 prefix list sequence number of entry.

*instance*

Specifies an IPv6 prefix list instance number.

## Modes

Global configuration mode

## Usage Guidelines

An IPv6 prefix list is composed of one or more conditional statements that execute a permit or deny action if a route matches a specified prefix. In prefix lists with multiple statements, you can specify a sequence number for each statement. The specified sequence number determines the order in which the statement appears in the prefix.

You can configure an IPv6 prefix list on a global basis, then use it as input to other commands or processes, such as route aggregation, route redistribution, route distribution, route maps, and so on. When an SLX-OS device interface sends or receives an IPv6 packet, it applies the statements within the IPv6 prefix list in their order of appearance to the packet. As soon as a match occurs, the device takes the specified action (permit or deny the packet) and stops further comparison for that packet.

You can use permit statements in the prefix list to specify the traffic that you want to send to the other feature. If you use deny statements, the traffic specified by the deny statements is not supplied to the other feature. You can configure up to one hundred IPv6 prefix lists.

You must specify the `ipv6-prefix` parameter in hexadecimal using 16-bit values between colons as documented in RFC 4291. You must specify the `prefix-length` parameter as a decimal value. A slash mark (/) must follow the `ipv6-prefix` parameter and precede the `prefix-length` parameter.

The *ge-value* or *le-value* you specify must meet the following condition for *prefix-length*:

```
ge-value <= le-value <= 128
```

## Examples

The following example creates a prefix-list that allows routes with the prefix 2001:db8::/32 .

```
device# configure terminal
device(config)# ipv6 prefix-list route1 permit 2001:db8::/32
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# ipv6 prefix-list route1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 protocol vrrp

Globally enables IPv6 VRRPv3.

## Syntax

`ipv6 protocol vrrp`

`no ipv6 protocol vrrp`

## Command Default

IPv6 VRRPv3 is not enabled.

## Modes

Global configuration mode

## Usage Guidelines

The **no** form of this command globally disables VRRPv3.

## Examples

To enable IPv6 VRRPv3 globally:

```
device# configure terminal
device(config)# ipv6 protocol vrrp
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 protocol vrrp-extended

Globally enables IPv6 VRRP-Ev3.

## Syntax

```
ipv6 protocol vrrp-extended
```

```
no ipv6 protocol vrrp-extended
```

## Command Default

IPv6 VRRP-Ev3 is disabled.

## Modes

Global configuration mode

## Usage Guidelines

The **no** form of this command globally disables IPv6 VRRP-Ev3.

## Examples

To enable IPv6 VRRP-Ev3 globally:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 receive access-group

Applies an IPv6 access control list (ACL) at global configuration level. Such *receive-path* ACLs filter incoming route-processor traffic according to rules that you create, but do not filter data-path traffic.

## Syntax

```
ipv6 receive access-group acl-name
```

```
no ipv6 receive access-group acl-name
```

## Command Default

No receive-path ACLs are applied.

## Parameters

*acl-name*

Specifies the name of the standard or extended IP access list.

## Modes

Global configuration mode

## Usage Guidelines

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL, from an interface-subtype configuration mode you use the { **ip** | **ipv6** | **mac** } **access-group** command.
- To apply a receive-path ACL, from global configuration mode you use the { **ip** | **ipv6** } **receive access-group** command.

You can apply a maximum of two receive-path ACLs to a device, as follows:

- One IPv4 receive-path ACL
- One IPv6 receive-path ACL

To remove a receive-path ACL, enter the **no** form of this command.

## Examples

The following example creates an IPv6 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ipv6 access-list extended ipv6-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10::1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20::1 count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq bgp count

device(conf-ipacl-ext)# exit
device(config)# ipv6 receive access-group ipv6-receive-acl-example
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 route

Configures an IPv6 static route.

## Syntax

```
ipv6 route dest-ipv6-prefix/prefix-length next-hop-ipv6-address [ metric ] [ distance number ] [ tag tag-number ]
```

```
ipv6 route dest-ipv6-prefix/prefix-length link-local-next-hop-ipv6-address [ ve ve-id ] [ metric ] [ distance number ] [ tag tag-number ]
```

```
ipv6 route dest-ipv6-prefix/prefix-length link-local-next-hop-ipv6-address [ ethernet slot/port ] [ metric ] [ distance number ] [ tag tag-number ]
```

```
no ipv6 route dest-ipv6-prefix/prefix-length next-hop-ipv6-address
```

```
no ipv6 route dest-ipv6-prefix/prefix-length link-local-next-hop-ipv6-address [ ve ve-id ]
```

```
no ipv6 route dest-ipv6-prefix/prefix-length link-local-next-hop-ipv6-address [ ethernet slot/port ]
```

## Command Default

No IPv6 static route is configured by default.

## Parameters

*dest-ipv6-prefix*

Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

*prefix-length*

A decimal value specifying the length of the IPv6 address prefix.

*next-hop-ipv6-address*

IPv6 address of the next-hop gateway.

*link-local-next-hop-ipv6-address*

IPv6 address of the link-local next-hop gateway.

**ethernet** *slot/port*

Specifies the Ethernet slot and port.

**ve** *ve-id*

Specifies the virtual Ethernet (VE) interface.

*metric*

Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

**distance** *number*

Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route,



configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

#### tag

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

#### *tag-number*

A number from 0 through 4294967295. The default is 0.

## Modes

Global configuration mode

VRF configuration mode

## Usage Guidelines

Use the **no** form of the command with the same parameters to remove the IPv6 static route.

## Examples

The following example creates an IPv6 static route for a destination network with the prefix 2001:DB8::0/32 and a next-hop gateway with the global address 2001:DB8:0:ee44::1.

```
device# configure terminal
device(config)# ipv6 route 2001:DB8::0/32 2001:DB8:0:ee44::1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 route next-hop-vrf

Configures an IPv6 static route through a named VRF.

## Syntax

```
ipv6 route ipv6-prefix/prefix-length next-hop-vrf vrf_name next-hop-ipv6-address [metric] [distance number] [tag tag-number]
```

```
no ipv6 route ipv6-prefix/prefix-length next-hop-vrf vrf_name next-hop-ipv6-address
```

## Command Default

No IPv6 static route is configured by default.

## Parameters

*dest-ipv6-prefix*

Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

*prefix-length*

A decimal value specifying the length of the IPv6 address prefix.

*next-hop-ipv6-address*

IPv6 address of the next-hop gateway.

**next-hop-vrf** *vrf\_name* *next-hop-ipv6-address*

Specifies a VRF instance and a next-hop IPv6 address.

*metric*

Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

**distance** *number*

Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

**tag**

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

*tag-number*

A number from 0 through 4294967295. The default is 0.

## Modes

Global configuration mode

VRF configuration mode

## Usage Guidelines

Use the **no** form of the command with the same parameters to remove the IPv6 static route.

Related commands:

- **ipv6 route**
- **ipv6 route null**

## Examples

The following example creates an IPv6 static route to IPv6 2001:DB8::0/32 destinations through the VRF named "partners" and the next-hop router with the IPv6 address 2001:DB8:0:ee44::1.

```
device# configure terminal
device(config)# ipv6 route 2001:DB8::0/32 next-hop-vrf partners 2001:DB8:0:ee44::1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 route null

Configures an IPv6 null route for discarding traffic.

## Syntax

```
ipv6 route dest-ipv6-prefix/prefix-length null 0 [ metric ] [ distance number ] [ tag tag-number ]
no ipv6 route dest-ipv6-prefix/prefix-length null 0
```

## Command Default

No IPv6 static route is configured by default.

## Parameters

*dest-ipv6-prefix*

Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

*prefix-length*

A decimal value specifying the length of the IPv6 address prefix.

*next-hop-ipv6-address*

IPv6 address of the next-hop gateway.

**null 0**

Causes packets to the selected destination to be dropped by shunting them to the "null 0" interface. (This is the only available option.)

**ethernet** *slot/port*

Specifies the Ethernet slot and port.

*metric*

Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

**distance** *number*

Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

**tag**

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

*tag-number*

A number from 0 through 4294967295. The default is 0.

## Modes

Global configuration mode

VRF configuration mode

## Usage Guidelines

Use the **no** form of the command with the same parameters to remove the null route.

Related commands:

- **ipv6 route**
- **ipv6 route next-hop-vrf**

## Examples

The following example creates a primary route to all 2001 : DB8 : : 0/32 destinations through virtual interface (ve) 3. It creates an alternative null route to drop packets when the primary route is not available.

```
device# configure terminal
device(config)# ipv6 route 2001 : DB8 : : 0/32 fe80::1 ve 3
device(config)# ipv6 route 2001 : DB8 : : 0/32 null 0 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing at the interface level.

## Syntax

`ipv6 router isis`

## Command Default

Disabled.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **no** form of the command disables IS-IS routing for the interface.

## Examples

The following example enables IS-IS routing for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 router isis
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 router ospf

Enables and configures the Open Shortest Path First version 3 (OSPFv3) routing protocol.

## Syntax

```
ipv6 router ospf [ vrf name ]
no ipv6 router ospf
```

## Command Default

Disabled.

## Parameters

*vrf name*  
Specifies a nondefault VRF.

## Modes

Global configuration mode

## Usage Guidelines

If you save the configuration to the startup-config file after disabling OSPFv3, all OSPFv3 configuration information is removed from the startup-config file.

Use this command to enable the OSPFv3 routing protocol and enter OSPFv3 router or OSPFv3 router 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-ipv6-router-ospf-vrf-default-vrf)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 vrrp-extended auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol Extended (VRRP-E) interface.

## Syntax

```
ipv6 vrrp-extended auth-type md5-auth auth-text
no ipv6 vrrp-extended auth-type md5-auth
```

## Command Default

No authentication is configured for a VRRP-E interface.

## Parameters

**md5-auth** *auth-text*  
Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

## Modes

Virtual Ethernet (ve) interface configuration mode

## Usage Guidelines

This configuration is for virtual Ethernet (ve) interfaces only.

If the **md5-auth** option is configured, syslog and SNMP traps are generated if a packet is being dropped due to MD5 authentication failure. Using MD5 authentication implies that the software does not need to run checksum verification on the receiving device and can rely on the authentication code (message digest 5 algorithm) to verify the integrity of the VRRP-E message header.

The **no** form of this command removes the VRRP-E authentication from the interface.

## Examples

The following example configures MD5 authentication on Virtual Ethernet interface 20.

```
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 20
device(config-if-Ve-20)# ipv6 vrrp-extended auth-type md5-auth lyk28d3j
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ipv6 vrrp-extended-group

Configures an IPv6 VRRP-Ev3 group and enters into the VRRP-E configuration mode.

## Syntax

```
ipv6 vrrp-extended-group group-ID
no ipv6 vrrp-extended-group group-ID
```

## Parameters

*group-ID*

A number from 1 through 255 that you assign to the VRRP-Ev3 group.

## Modes

Virtual Ethernet (VE) interface configuration mode

## Usage Guidelines

Enter **no ipv6 vrrp-extended-group *group-ID*** to remove the specific IPv6 VRRP-Ev3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

This configuration is for virtual Ethernet (VE) interfaces only. IPv6 VRRP-Ev3 must be enabled on the device before the IPv6 VRRP-E group is configured.

## Examples

The following example shows how to assign the VE interface with a VLAN number of 2019 to the VRRP-Ev3 group with the ID of 19.

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 2019
device(config-Ve-2019)# ipv6 address 2001:2019:8192::122/64
device(config-Ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 vrrp-group

Configures an IPv6 VRRPv3 group and enters into the virtual router configuration mode.

## Syntax

```
ipv6 vrrp-group group-ID
```

```
no ipv6 vrrp-group group-ID
```

## Parameters

*group-ID*

A value from 1 through 255 that you assign to the VRRPv3 group.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Enter **no ipv6 vrrp-group** *group-ID* to remove a specific IPv6 VRRPv3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

IPv6 VRRPv3 must be enabled on the device before the IPv6 VRRP group is configured.

## Examples

The following example shows how to assign an Ethernet interface to the VRRPv3 group with the ID of 18.

```
device# configure terminal
device(config)# ipv6 protocol vrrp
device(config)# interface ethernet 1/6
device(config-if-eth-1/6)# ipv6 address 2001:2019:8192::125/64
device(config-if-eth-1/6)# ipv6 vrrp-group 18
device(config-vrrp-group-18)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ipv6 vrrp-suppress-interface-ra

Suppresses interface router advertisement (RA) when VRRPv3 is configured on an interface.

## Syntax

```
ipv6 vrrp-suppress-interface-ra
no ipv6 vrrp-suppress-interface-ra
```

## Command Default

Interface RA is enabled.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Enter **no ipv6 vrrp-suppress-interface-ra** to remove the suppression of interface RA.

Router advertisements are sent by the VRRP master device and contain the link-local virtual IP address and the virtual MAC address. For network security reasons, if you do not want the MAC addresses of interfaces to be viewed, you can disable RA messages.

## Examples

This example suppresses interface RA on a virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# ipv6 protocol vrrp
device(config)# interface ve 2019
device(config-Ve-2019)# ipv6 vrrp-suppress-interface-ra
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis auth-check

Enables authentication checking for an IS-IS interface.

## Syntax

```
isis auth-check { level-1 | level-2 } disable  
no isis auth-check { level-1 | level-2 } disable
```

## Command Default

ISIS authentication checking is enabled by default.

## Parameters

**level-1**  
Specifies Level 1 packets.

**level-2**  
Specifies Level 2 packets.

**disable**  
Disables authentication checking.

## Modes

Interface subtype configuration mode

## Usage Guidelines

no

## Examples

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

```
device# configure terminal  
device(config)# interface ethernet 1/1  
device(conf-if-eth-1/1)# isis auth-check disable
```

The following example re-enables IS-IS authentication checking for Level 2 packets for an IS-IS loopback interface.

```
device# configure terminal  
device(config)# interface loopback 1  
device(config-loopback-1)# isis auth-check
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis auth-key

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

## Syntax

```
isis auth-key { level-1 | level-2 } string
```

```
no isis auth-key { level-1 | level-2 } string
```

## Command Default

Disabled.

## Parameters

### level-1

Specifies Level 1 packets only.

### level-2

Specifies Level 2 packets only.

### string

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

## Modes

Interface subtype configuration mode

## Usage Guidelines

The authentication mode must be configured on the interface using the **isis auth-mode** command before a *string* can be configured. If the authentication mode is reset, the authentication key must also be reset.

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

## Examples

The following example configures an authentication key for Level 1 packets on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis auth-key level-1 mykey
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis auth-mode

Specifies the type of authentication used for an Intermediate System-to-Intermediate System (IS-IS) interface.

## Syntax

```
isis auth-mode md5 { level-1 | level-2 }
```

```
no isis auth-mode md5 { level-1 | level-2 }
```

## Command Default

Disabled.

## Parameters

**md5**

Specifies message Digest 5 (MD5) authentication.

**level-1**

Specifies Level 1 packets only.

**level-2**

Specifies Level 2 packets only.

## Modes

Interface subtype configuration mode

## Usage Guidelines

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

## Examples

The following example specifies that MD5 authentication is performed on Level 1 packets on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis auth-mode MD5 level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis circuit-type

Configures the type of adjacency used for an Intermediate System-to-Intermediate System (IS-IS) interface.

## Syntax

```
isis circuit-type { level-1 | level-1-2 | level-2 }
```

```
no circuit-type { level-1 | level-1-2 | level-2 }
```

## Command Default

Level 1 and Level 2 adjacency is configured by default.

## Parameters

### level-1

Specifies Level 1 packets only.

### level-1-2

Specifies Level 1 and Level 2 packets.

### level-2

Specifies Level 2 packets only.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **no** form of the command resets the type of adjacency to the default value of Level 1 and Level 2 adjacency.

## Examples

The following example configures Level 1 adjacency on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# isis circuit-type level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# isis hello-interval

Specifies how often an Intermediate System-to-Intermediate System (IS-IS) interface sends hello messages to its IS-IS neighbors.

## Syntax

```
isis hello-interval { level-1 | level-2 } value
```

```
no isis hello-interval { level-1 | level-2 } value
```

## Command Default

Disabled.

## Parameters

### level-1

Configures the hello interval for Level 1 only.

### level-2

Configures the hello interval for Level 2 only.

### value

Specifies the interval. Valid values range from 1 through 63 seconds. The default is 10.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **no** form of the command resets the hello interval to the default value of 10 seconds.

## Examples

The following example changes the hello interval for Level 1 packets to 20 on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# isis hello-interval level-1 20
```

The following example changes the hello interval for Level 2 packets to 40 on a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-loopback-1)# isis hello-interval level-2 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis hello-multiplier

Specifies the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the device declares adjacency as down.

## Syntax

```
isis hello-multiplier { level-1 | level-2 } multiplier
```

```
no isis multiplier { level-1 | level-2 } multiplier
```

## Command Default

The default is 3.

## Parameters

### level-1

Configures the hello multiplier for Level 1 adjacencies.

### level-2

Configures the hello multiplier for Level 2 adjacencies.

### multiplier

Specifies the multiplier. Valid values range from 3 through 1000. The default is 3.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The hello multiplier is the number by which an IS-IS interface multiplies the hello interval to obtain the hold time for Level-1 and Level-2 IS-IS hello PDUs.

The **no** form of the command restores the default of 10 seconds.

## Examples

The following example changes the hello multiplier for Level 1 packets for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# isis hello-multiplier level-1 10
```

The following example changes the hello multiplier for Level 2 packets for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-loopback-1)# isis hello-multiplier level-2 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis hello padding

Re-enables Intermediate System-to-Intermediate System (IS-IS) hello padding at the interface level.

## Syntax

```
isis hello padding [ disable ]
no isis hello padding [ disable ]
```

## Command Default

IS-IS hello padding is enabled.

## Parameters

**disable**  
Disables hello padding on the interface.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Generally, you do not need to disable padding unless a link is experiencing slow performance. If you enable or disable padding on an interface, the interface setting overrides the global setting configured using the **hello padding** command.

The **no** form of the command disables hello padding.

## Examples

The following example re-enables IS-IS hello padding on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# isis hello padding
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis ipv6 metric

Configures the metric value for an interface under IPv6 Intermediate System-to-Intermediate System (IS-IS) MT.

## Syntax

```
isis ipv6 metric { level-1 | level-2 } metric
```

```
no ipv6 metric { level-1 | level-2 } metric
```

## Command Default

The default is 10.

## Parameters

### level-1

Specifies Level 1 only.

### level-2

Specifies Level 2 only.

### multiplier

Specifies the metric value. Valid values range from 1 through 16777215. The default is 10.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Each IS-IS interface has a separate metric value. In IPv6 IS-IS MT, different metrics are configured on an interface for IPv4 and IPv6. When the metric value is configured for an interface, it rebuilds the route LSP and triggers IPv6 IS-IS MT SPF calculation.

The **no** form of the command resets the metric value to the default value of 10.

## Examples

The following example changes the metric value for Level 1 packets for an Ethernet interface under IPv6 IS-IS MT to 25.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# isis ipv6 metric level-1 25
```

The following example changes the metric value for Level 2 packets for a loopback interface under IPv6 IS-IS MT to 60.

```
device# configure terminal
device(config)# interface loopback 1
device(config-loopback-1)# isis ipv6 metric level-2 60
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis ldp-sync

Enables synchronization with Intermediate System-to-Intermediate System (IS-IS) for an interface.

## Syntax

```
isis ldp-sync { disable | enable}
```

```
no isis ldp-sync { disable | enable}
```

## Command Default

Disabled.

## Parameters

disable

Disables LDP synchronization.

enable

Enables LDP synchronization.

## Modes

Interface subtype configuration mode

## Examples

The following example enables LDP synchronization for an ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis ldp-sync enable
```

The following example disables LDP synchronization for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# isis ldp-sync disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# isis metric

Configures the value of an Intermediate System-to-Intermediate System (IS-IS) metric.

## Syntax

```
isis metric { level-1 | level-2 } metric
```

```
no metric { level-1 | level-2 } metric
```

## Command Default

The default is 10.

## Parameters

### level-1

Specifies Level 1 only.

### level-2

Specifies Level 2 only.

### metric

Specifies the metric. Valid values range from 1 through 63 for the narrow metric style (the default metric style for IPv4 ISIS). Valid values range from 1 through 16777215 for the wide metric style (the default metric style for IPv4 ISIS).

## Modes

Interface subtype configuration mode

## Usage Guidelines

Each IS-IS interface has a separate metric value.

The device applies the interface-level metric to routes originated on the interface and when calculating routes. The device does not apply the metric to link-state information received from one intermediate system and flooded to other intermediate systems.

If the metric value you want to use is higher than 63 but you have not changed the metric style to wide, you must change the metric style first, and then set the metric. The IS-IS neighbors that receive the advertisements must also be enabled to receive wide metrics.

The **no** form of the command resets the metric value the default value of 10.

## Examples

The following example changes the metric for an Ethernet interface, specifying Level 1 packets.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis metric 25 level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis passive

Disables adjacency formation and advertisements on an Intermediate System-to-Intermediate System (IS-IS) interface.

## Syntax

**isis passive**

**no isis passive**

## Command Default

Adjacency formation and advertisements is disabled on loopback interfaces. Adjacency formation and advertisements is enabled on all other interfaces.

## Modes

Interface subtype configuration mode

## Usage Guidelines

A device advertises an IS-IS interface to its area regardless of whether adjacency formation is enabled.

The **no** form of the command re-enables adjacency formation and advertisements on the IS-IS interface.

## Examples

The following example disables adjacency formation and advertisements on an Ethernet interface.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# isis passive
```

The following example enables adjacency formation and advertisements on a loopback interface.

```
device#configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# no isis passive
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis point-to-point

Configures the network type for the Intermediate System-to-Intermediate System (IS-IS) interface as point-to-point.

## Syntax

**isis point-to-point**

**no isis point-to-point**

## Command Default

Disabled.

## Modes

Interface subtype configuration mode

## Usage Guidelines

The **no** form of the command removes the configured point-to-point network type.

## Examples

The following example configures a network type of point-to-point for an Ethernet interface.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# isis point-to-point
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis priority

Determines the priority of the interface for being elected as a Designated IS.

## Syntax

```
isis priority { level-1 | level-2 } value
```

```
no isis priority { level-1 | level-2 } value
```

## Command Default

The default is 64.

## Parameters

### level-1

Sets the priority for Level 1 only.

### level-2

Sets the priority for Level 2 only.

### value

Specifies the priority. Valid values range from 0 through 127. The default is 64.

## Modes

Interface subtype configuration mode

## Usage Guidelines

You can configure the same priority for both Level-1 and Level-2 or you can configure a different priority for each level. If two or more devices have the highest priority within a given level, the device with the highest MAC address becomes the Designated IS for that level.

You can set the IS-IS priority on an individual interface basis only. You cannot set the priority globally.

The **no** form of the command resets the priority value to the default value of 64.

## Examples

The following example changes the priority for Level 1 packets for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis priority level-1 100
```

The following example changes the hello multiplier for Level 2 packets for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# isis priority level-2 80
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# isis reverse-metric

Configures the reverse metric value on a single Intermediate System-to-Intermediate System (IS-IS) interface.

## Syntax

```
isis reverse-metric [ value ] [ te-def-metric ] [ whole-lan ]  
no isis reverse-metric [ value ] [ te-def-metric ] [ whole-lan ]
```

## Command Default

Disabled.

## Parameters

*value*

Specifies the reverse metric value in metric style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default value is 16777214 irrespective of the metric style configured.

**whole-lan**

Specifies that the configured reverse metric value affects the entire LAN.

**te-def-metric**

Specifies that the device sends a traffic engineering (TE) default metric sub-type-length-value (TLV) within the reverse metric TLV.

## Modes

Interface subtype configuration mode

## Usage Guidelines

If the reverse metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor 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.

If the **whole-lan** option is not enabled, the reverse metric value affects only the neighbor router. The **whole-lan** option takes effect only on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the **whole-lan** option is enabled.

The **no** form of the command removes the entire reverse metric configuration. The **no** form of the command specified with the configured value resets the metric value to the default value of 16777214.

## Examples

The following example configures a reverse metric value of 40 on an Ethernet interface. The **whole-lan** option is enabled to include the entire LAN.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# isis reverse-metric 40 whole-lan
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# is-type

Changes the Intermediate System-to-Intermediate System (IS-IS) level globally.

## Syntax

```
is-type { level-1 | level-1-2 | level-2 }
no is-type { level-1 | level-1-2 | level-2 }
```

## Command Default

The device operates as both a Level 1 (intra-area) and a Level 2 (interarea) device.

## Parameters

- level-1**  
Specifies that the device performs only Level 1 (intra-area) routing.
- level-1-2**  
Specifies that the device performs both Level 1 and Level 2 routing.
- level-2**  
Specifies that the device performs only Level 2 (interarea) routing.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command enables support for both IS-IS levels, if one level has been disabled. Alternatively, the **level-1-2** parameter can be used.

## Examples

The following example changes the IS-IS level globally to Level-1 only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-1
```

The following example changes the IS-IS level globally to Level-2 only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-2
```

The following example changes the IS-IS level globally to Level-1 and Level-2 if support for one level has previously been disabled.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-1-2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# iterations

For an implementation of an event-handler profile, specifies the number of times an event-handler action is run, when triggered.

## Syntax

**iterations** *num-iterations*

**no iterations**

## Command Default

When the trigger condition occurs, the event-handler actions runs once.

## Parameters

*num-iterations*

Specifies the number of times an event-handler action is run, when triggered. Valid values are any positive integer.

## Modes

Event-handler activation mode

## Usage Guidelines

The **no** form of this command resets the **iterations** setting to the default 1 iteration.

## Examples

The following example specifies 5 iterations.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# iterations 5
```

The following example resets **iterations** to the default value of 1 iteration.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no iterations
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# Commands K - M

---

## ka-int-count

Configures the number of keepalive intervals after which the session is terminated when no session keepalive or other LDP protocol message is received from the LDP peer.

### Syntax

**ka-int-count** *number*

**no ka-int-count** *number*

### Command Default

The default is a count of six intervals.

### Parameters

*number*

Specifies the number of keepalive time intervals. Enter an integer from 1 to 65535.

### Modes

MPLS LDP configuration mode

### Usage Guidelines

Use the **no** form of the command to reset the default count of six intervals.

### Examples

The following example configures a keepalive interval count of three.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# ka-int-count 3
```

### History

Release version	Command history
16r.1.00	This command was introduced.

# ka-interval

Sets the keepalive time interval at which the session keepalive message is sent when no other LDP protocol message is sent to the LDP peer.

## Syntax

**ka-interval** *seconds*

**no ka-interval** *seconds*

## Command Default

The default is six seconds.

## Parameters

*seconds*

Specifies the keepalive time interval in seconds. Enter an integer from 1 to 65535.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

The **ka-interval** and the **ka-timeout** configurations are mutually exclusive and you may have only one configured at a time. You must explicitly remove the configuration for one in order to change to the other configuration.

When the keepalive timeout value is configured, the **show mpls ldp** command displays keepalive interval as keepalive timeout divided by the keepalive interval count (ka-timeout/ka-in-count).

A message is displayed whenever the **ka-interval** value is changed.

```
"Please clear LDP sessions for the new KA parameter value to take effect on existing sessions"
```

Use the **no** form of the command to reset the default of six seconds.

## Examples

The following example configures a keepalive interval of 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# ka-interval 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ka-timeout

Sets the keepalive timeout after which the session is terminated when the keepalive or LDP protocol message is not received.

## Syntax

**ka-timeout** *seconds*

**no ka-timeout** *seconds*

## Command Default

The default is six seconds.

## Parameters

*seconds*

Specifies the keepalive timeout in seconds. Enter an integer from 1 to 65535.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

After an LDP session is established, an LSR maintains the integrity of the session by sending keepalive messages. The keepalive timer for each peer session resets whenever it receives any LDP protocol message or a keepalive message on that session. When the keepalive timer expires, LDP concludes that the TCP connection is bad or the peer is dead and terminates the session.

When the keepalive timeout value is configured, the **show mpls ldp** command displays keepalive interval as keepalive timeout divided by the keepalive interval count (ka-timeout/ka-in-count).

The **ka-interval** and the **ka-timeout** configurations are mutually exclusive and you may have only one configured at a time. You must explicitly remove the configuration for one in order to change to the other configuration.

A message is displayed whenever the **ka-timeout** value is changed.

```
"Please clear LDP sessions for the new KA parameter value to take effect on existing sessions"
```

Use the **no** form of the command to reset the default timeout of six seconds.

## Examples

The following example configures a keepalive timeout of 180 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# ka-timeout 180
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# key-add-remove-interval

Alters the timing of the authentication key add-remove interval.

## Syntax

**key-add-remove-interval** *interval*

**no key-add-remove-interval** *interval*

## Command Default

The interval is 300 seconds.

## Parameters

*interval*

Specifies the add-remove interval in seconds. Valid values range from 0 through 14400. The default is 300.

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

The **no** form of the command sets the add-remove interval to the default value of 300 seconds.

## Examples

The following example sets the key add-remove interval to 240 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# key-add-remove-interval 240
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# key-rollover-interval

Alters the timing of the existing configuration changeover.

## Syntax

```
key-rollover-interval interval
```

```
no key-rollover-interval interval
```

## 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-ipv6-router-ospf-vrf-default-vrf)# key-rollover-interval 420
```

The following example re-sets the key rollover interval to the default value.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no key-rollover-interval 420
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# keypair

Associates the generated RSA/ECDSA/DSA key pair with a trust point for security protocol exchanges for applications.

## Syntax

Associates the generated RSA/ECDSA/DSA key pair with the trust point.

**keypair** *key\_label*

**no keypair**

## Parameters

*key\_label*

Specifies the name of the key pair to associate with the trust point.

## Modes

Trust point configuration mode

## Usage Guidelines

Use the **no keypair** command to remove the key pair association.

## Examples

Typical command usage:

```
device(config)# crypto ca trustpoint t1
device(config-ca-t1)# keypair k1
device(config-ca-t1)# do show running-config crypto
crypto key label k1 rsa modulus 2048
crypto ca trustpoint t1
keypair k1
!
device# show crypto ca trustpoint
trustpoint: t1; key-pair: k1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# 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**

## Command Default

The default is 60.

## Parameters

*secs*

Specifies the delay period in seconds for the label withdrawal delay timer. Enter value from 0 to 300.

## Modes

MPLS LDP configuration mode.

## Usage Guidelines

Setting the *secs* variable to zero (0) disables the feature for subsequent events.

Setting the *secs* variable to a value from 1 to 300, updates the configured value.

When using the **no** form of the command to restore the default behavior.

## Examples

The following example sets the label withdrawal delay timer to 30 seconds.

```
device(config-router-mpls-ldp)# label-withdrawal-delay 30
```

The following example restores the command default behavior.

```
device(config-mpls-router-ldp)# no label-withdrawal-delay
```

The following example disables the label withdrawal delay timer.

```
device(config-mpls-router-ldp)# label-withdrawal-delay 0
```

## History

Release	Command history
16r. 1.00	This command is introduced.

# Ldp

Enables the Label Distribution Protocol (LDP) mode to configure LDP global parameters.

## Syntax

```
ldp
no ldp
```

## Modes

MPLS configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the LDP configurations from the device.

## Examples

The following example enables LDP configuration mode.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# ldp-enable

Enables LDP on an interface.

## Syntax

**ldp-enable**

**no ldp-enable**

## Command Default

None

## Modes

MPLS interface configuration mode

## Usage Guidelines

For an LDP session between routers, you must configure LDP on an interface to allow the device to advertise its loopback interface to the peers.

To use LDP, configure a loopback address with a 32-bit mask on the LSR. The first loopback address configured on the device is used in its LDP identifier. When the loopback address used in the LDP identifier is removed, all LDP functions on the LSR are shut down. LDP sessions between the LSR and its peers are terminated, and LDP-created tunnels are removed. When other loopback interfaces are configured on the device, the lowest-numbered loopback address is used as a new LDP identifier. LDP sessions and tunnels are set up using this new LDP identifier.

Configure LDP on the same set of interfaces that IGP routing protocols such as OSPF and IS-IS are enabled.

Use the **no** form of the command to disable LDP on the interface.

## Examples

The following example configures LDP on an interface.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/2
device(config-router-mpls-interface-1/2)# ldp-enable
```

## History

Release version	Command history
16r. 1.00	This command was introduced.



# ldp-params

Allow you to access ldp-params subconfiguration mode to configure LDP parameters on an interface.

## Syntax

```
ldp-params
no ldp-params
```

## Command Default

None

## Modes

MPLS interface configuration mode

## Usage Guidelines

When you use this command, you can configure the LDP Hello interval and timeout parameters on the interface.

Use the **no** form of the command to remove the LDP parameter configuration.

## Examples

The following example accesses ldp-params subconfiguration mode.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/2
device(config-router-mpls-interface-1/2)# ldp-params
device(config-router-mpls-interface-1/2-ldp-params)#
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# ldp-sync

Enables Multiprotocol Label Switching (MPLS) Label Distribution Protocol-Interior Gateway Protocol (LDP-IGP) synchronization globally with Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), and configures the hold-down time interval.

## Syntax

```
ldp-sync [ hold-down seconds ]
```

```
no ldp-sync [ hold-down ]
```

## Command Default

Disabled.

## Parameters

**hold-down** *seconds*

Sets the LDP-IGP synchronization hold-down time interval in seconds. The IGP must advertise the maximum IP metric while waiting for an update from the LDP. Valid values range from 1 through 65535 seconds. The default is 30.

## Modes

OSPF router configuration mode

IS-IS address-family IPv4 unicast configuration mode

## Usage Guidelines

The **ldp-sync** command supports point-to-point interfaces, but not tunnel interfaces.

This command affects IPv4 metrics only.

When enabled on IS-IS, consider the following:

- The feature applies to both level-1 and level-2 metrics.
- The wide metric-style is required.

The **no ldp-sync** command disables LDP-IGP synchronization.

The **no ldp-sync hold-down** command resets the hold down time interval to the default setting of 30 seconds.

## Examples

The following example enables MPLS LDP-IGP synchronization globally with OSPF and IS-IS, and sets the hold-down time interval to 100 seconds.

```
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# ldp-sync
device(config-router-ospf-vrf-default-vrf)# ldp-sync hold-down 100
device(config-router-ospf-vrf-default-vrf)# exit
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# metric-style wide
device(config-router-isis-ipv4u)# ldp-sync
device(config-router-isis-ipv4u)# ldp-sync hold-down 100
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# link-error-disable

Configures port flap dampening for the interface, including the threshold of link flapping to shut down the port and the time interval in which it remains shut down.

## Syntax

**link-error-disable** *toggle-threshold sampling-time-in-sec wait-time-in-sec*

**no link-error-disable**

## Command Default

Port flap dampening is disabled on the device.

## Parameters

*toggle-threshold*

Specifies the number of times a port link state goes from up to down and down to up before the wait period is activated. The value ranges from 1 through 50.

*sampling-time-in-sec*

Specifies the amount of time, in seconds, during which the specified toggle threshold can occur before the wait period is activated. Enter an integer from 1 through 65535.

*wait-time-in-sec*

Specifies the amount of time, in seconds, for which the port remains disabled (down) before it becomes enabled. The value ranges from 0 through 65535. A value of 0 indicates that the port will stay down until an administrative override occurs.

## Modes

Interface Ethernet configuration mode

## Usage Guidelines

Use the **no** form of the command to disable port flap dampening.

Port flap dampening allows you to configure a wait period before a port, whose link goes down then up, becomes enabled. This feature is available for all front ports on the device.

If the port link state toggles, from down to up or from up to down, for a specified number of times within a specified period, the interface is physically disabled for the specified wait period. Once the wait period expires, the port's link state is re-enabled. However, if the wait period is set to zero (0) seconds, or you want to re-enable the port before the wait period expires, the port must be manually re-enabled. To re-enable the port, reenter the **link-error-disable** command on the disabled port.

## Examples

The following example shows the configuration of port flap dampening. The toggle threshold is set to 10 times. The sampling time is set to 3 seconds. The wait time is set to 10 seconds.

```
device# configure terminal
device(config)# interface Ethernet 1/4
device(conf-if-eth-1/4)# link-error-disable 10 3 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# link-fault-signal

Configures RX and TX Link Fault Signaling (LFS) detection globally or on an interface port.

## Syntax

```
link-fault-signal rx { off | on } tx { off | on
no link-fault-signal
```

## Command Default

Both TX and RX LFS are enabled.

## Parameters

<b>rx</b>	Configure RX LFS detection.
<b>off</b>	Disables LFS.
<b>on</b>	Enables LFS.
<b>tx</b>	Configure TX LFS detection.

## Modes

Global and interface configuration modes

## Usage Guidelines

Use the **no** form of the command to reset RX and TX LFS to their default settings of enabled.

The interface must be in the shutdown state before you disable or enable TX LFS.

The SLX 9850 supports LFS detection for interface types of 10G, 40G, 100G, and 40G breakout ports. It detects local and remote faults.

LFS is not supported in 1G mode.

When the device detects a local fault, it returns a remote fault to the link partner. When the device detects a remote fault, it returns an idle state.

A port's physical link detection is independent of LFS detection. When either of these link fault signals is detected, the following behaviors occur:

- The link is declared as DOWN and the MM should display Protocol Down on the SLX-OS CLI.
- The physical link is not brought down in both of the previous cases. The peer side based on its implementation might display that the link is UP when the device displays that the link is DOWN due to a fault detection.

- The transmit (TX) packets, if any, are dropped at the MAC layer. The receive (RX) packets, if any, are dropped in the software.
- The detected signal is reported as a RASTRACE message on the line card. The same information is reported on the MM as a RASLOG. The same behavior occurs when the signal is cleared.

You can enable or disable LFS globally and on the interface level for both RX and TX directions:

- If the LFS is enabled for RX, the normal local and remote fault detection and processing described previously occur. If it is disabled for RX, local and remote fault detection are ignored.
- If the LFS is enabled for TX and a local fault occurs, a remote fault (pause frame) is generated to the remote side. If it is disabled for TX, the remote fault is not generated.

The interface configuration overrides the global configuration.

## Examples

The following example shows the global and interface configuration of LFS. In this example, the global LFS is disabled for the link fault RX and enabled for link fault TX. The LFS for the interface is enabled for the link fault RX and disabled for the link fault TX, overriding the global configuration.

```
device# configure terminal
device(config)# link-fault-signaling rx off tx on
device(config)# interface Ethernet 2/1
device(conf-if-eth-2/1)# shutdown
device(conf-if-eth-2/1)# link-fault-signaling rx on tx off
device(conf-if-eth-2/1)# no shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# load-sharing

Configures the maximum number of LDP ECMP paths.

## Syntax

`load-sharing number`

`no load-sharing`

## Command Default

The default number of ECMP paths is one.

## Parameters

*number*

Specifies the maximum number of LDP ECMP paths. Enter an integer from 1 to 16.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

The number of LDP ECMP paths for transit LSR depends on the number of eligible paths that are available, and the maximum number of LDP ECMP paths that you can configure.

Use the **no** form of this command to reset the default of one.

## Examples

The following example configures a maximum of four LDP ECMP paths.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# load-sharing 4
```

## History

Release version	Command history
16r. 1.00	This command was introduced.



# local-as

Specifies the BGP autonomous system number (ASN) where the device resides.

## Syntax

**local-as** *num*

**no local-as** *num*

## Command Default

No ASN is specified.

## Parameters

*num*

The local ASN. The range is from 1 through 4294967295.

## Modes

BGP configuration mode

## Usage Guidelines

ASNs in the range from 64512 through 65535 are private numbers that are not advertised to the external community.

The **no** form of the command removes the ASN from the device.

## Examples

This example assigns a separate local AS number.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 777
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# local-switching

Configures the local switching mode for a bridge domain.

## Syntax

`local-switching`  
`no local-switching`

## Command Default

Local switching is enabled.

## Parameters

`local-switching`  
 Enables local switching.

## Modes

Bridge-domain configuration mode.

## Usage Guidelines

Local switching allows packets to be switched within a VPLS bridge domain. This command only applies to multipoint-service bridge domains; that is, bridge domains configured with the **p2mp** option.

The **no** form of the command disables local switching in a VPLS bridge domain.

To avoid receipt of traffic with different VLAN tags on local endpoints in a bridge domain that has a PW profile with VC mode set to **raw-passthrough**, it is recommended that local switching is disabled. Raw passthrough mode is designed to forward packets between two VPLS peer devices and is not intended for use with local switching.

## Examples

The following example disables local switching in VPLS bridge domain 10.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# no local-switching
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# log (OSPFv2)

Controls the generation of OSPFv2 logs.

## Syntax

```
log { adjacency [ dr-only ] | all | bad-packet [ checksum ] | database | retransmit }
```

```
no log { adjacency [ dr-only ] | all | bad-packet [ checksum ] | database | retransmit }
```

## Command Default

Disabled. Only OSPFv2 messages indicating possible system errors are logged.

## Parameters

### adjacency

Specifies the logging of essential OSPFv2 neighbor state changes.

### dr-only

Specifies the logging of essential OSPF neighbor state changes where the interface state is designated router (DR).

### all

Specifies the logging of all syslog messages.

### bad-packet

Specifies the logging of bad OSPFv2 packets.

### checksum

Specifies all OSPFv2 packets that have checksum errors.

### database

Specifies the logging of OSPFv2 LSA-related information.

### retransmit

Specifies the logging of OSPFv2 retransmission activities.

## Modes

OSPF router configuration mode

OSPF VRF router configuration mode

## Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv2. If this command is not enabled only OSPFv2 messages indicating possible system errors are logged.

A limitation with the **dr-only** sub-option is that when a DR/BDR election is underway, OSPF neighbor state changes pertaining to non-DR/BDR routers are not logged. Logging resumes once a DR is elected on that network.

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

## Examples

The following example enables the logging of all OSPFv2-related syslog events.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# log all
```

The following example enables the logging of OSPFv2 retransmission activities.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# log retransmit
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# log (OSPFv3)

Controls the generation of OSPFv3 logs.

## Syntax

```
log { adjacency [ dr-only ] | all | bad-packet [ checksum ] | database | retransmit }
no log { adjacency | all | bad-packet [ checksum ] | database | retransmit }
```

## Command Default

Disabled. Only OSPFv3 messages indicating possible system errors are logged.

## Parameters

### adjacency

Specifies the logging of essential OSPFv3 neighbor state changes.

### dr-only

Specifies the logging only of designated router (DR) interface adjacency changes.

### all

Specifies the logging of all syslog messages.

### bad-packet

Specifies the logging of bad OSPFv3 packets.

### checksum

Specifies all OSPFv3 packets that have checksum errors.

### database

Specifies the logging of OSPFv3 LSA-related information.

### retransmit

Specifies the logging of OSPFv3 retransmission activities.

## Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

## Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv3. If this command is not enabled, only OSPFv3 messages indicating possible system errors are logged.

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

## Examples

The following example enables the logging of all OSPFv3-related syslog events.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# log all
```

The following example enables the logging of OSPFv3 retransmission activities.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# log retransmit
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# log adjacency

Logs changes in the status of an adjacency with another intermediate system (IS).

## Syntax

**log adjacency**

**no log adjacency**

## Command Default

Disabled.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command disables the logging of adjacency changes.

## Examples

The following example enables logging of adjacency changes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# log adjacency
```

The following example disables logging of adjacency changes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no log adjacency
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# log-dampening-debug

Logs dampening debug messages.

## Syntax

```
log-dampening-debug
no log-dampening-debug
```

## Command Default

This option is disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

The following example logs dampening debug messages.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# log-dampening-debug
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# log invalid-lsp-packets

Logs invalid Link State PDUs (LSPs) packets.

## Syntax

**log invalid-lsp-packets**

**no log invalid-lsp-packets**

## Command Default

Disabled.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command disables the logging of invalid LSP packets.

## Examples

The following example enables logging of invalid LSP packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# log invalid-lsp-packets
```

The following example disables logging of invalid LSP packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no log invalid-lsp-packets
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# log-shell

Controls the remote logging of SLXVM Linux shell command activities.

## Syntax

```
log-shell { start | status | stop }
```

## Command Default

By default, the device logs the SLXVM Linux shell access and all commands executed at the SLXVM Linux shell locally.

## Parameters

### start

Restarts remote logging.

### status

Checks the remote logging status.

### stop

Disables remote logging.

## Modes

Privileged EXEC mode

## Usage Guidelines

Changes of the **log-shell stop** and **log-shell start** commands are applicable only on new SLXVM Linux shell sessions.

If you configure a remote Syslog server, the same logs can be seen on this server.

When you disable remote logging, local logging of user activities continues.

## Examples

The following example disables remote logging.

```
device# log-shell stop
```

The following example restarts remote logging.

```
device# log-shell start
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# logical-interface (bridge domain)

Binds a logical interface to a bridge domain.

## Syntax

```
logical-interface { ethernet num | port-channel num }
```

```
logical-interface { ethernet num | port-channel num }
```

## Command Default

No interface is bound to the bridge domain.

## Parameters

**ethernet** *num*

Specifies an instance ID for an Ethernet logical interface.

**port-channel** *num*

Specifies an instance ID for a port-channel logical interface.

## Modes

Bridge-domain configuration mode.

## Usage Guidelines

The attachment circuit end-points (logical interfaces) bound to a bridge domain can be either regular Ethernet interfaces or LAG trunks (port-channels).

A logical interface must be created (by using the **logical interface** command in interface configuration mode) before it can be bound to a bridge domain.

The **no** version of the command removes the logical interface from the bridge domain configuration.

## Examples

The following example shows how to create a logical Ethernet interface instance ID (1/5.10) and bind to bridge domain 4.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# logical-interface ethernet 1/5.10
device(conf-if-eth-lif-1/5.10)# vlan 50
device(conf-if-eth-lif-1/5.10)# exit

device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/5.10
```

The following example shows how to bind a logical port-channel interface instance ID (2.200) to bridge domain 4.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface port-channel 2.200
```

The following example shows the error message that displays when an attempt is made to bind a logical interface that was not previously created, to a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/3.100
Error: Logical Interface not yet created
```

The following example shows the error message that displays when an attempt is made to bind a logical interface that is previously bound to another bridge domain.

```
device>enable
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/3.100
Error: LIF already Binded
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# lsp

Accesses LSP subconfiguration mode to configure the LSP tunnel.

## Syntax

**lsp** *name*

**no lsp** *name*

## Command Default

None

## Parameters

*name*

Specifies the name of the LSP tunnel.

## Modes

MPLS configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the LSP from the MPLS configuration.

## Examples

The following example configures LSP to2 and accesses LSP subconfiguration mode.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# lsp to2
device(config-router-mpls-lsp-to2)#
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# lsp-gen-interval

Sets the minimum number of seconds the device waits between sending updated Link State PDUs (LSPs) to its Intermediate System-to-Intermediate System (IS-IS) neighbors.

## Syntax

```
lsp-gen-interval interval
```

```
lsp-gen-interval interval
```

## Command Default

The default interval is 10 seconds.

## Parameters

*secs*

Specifies the interval in seconds. Valid values range from 0 through 120 seconds. The default is 10 seconds.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command removes the configured interval.

## Examples

The following example changes the LSP generation interval to 45 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-gen-interval 45
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# lsp-interval

Sets the rate of transmission, in milliseconds, of the Link State PDUs (LSPs).

## Syntax

**lsp-interval** *interval*

**lsp-interval** *interval*

## Command Default

The default interval is 33 milliseconds.

## Parameters

*secs*

Specifies the interval in milliseconds. Valid values range from 1 through 4294967295 milliseconds. The default is 33 milliseconds.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command removes the configured interval.

## Examples

The following example changes the LSP interval to 45 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-interval 45
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# lsp-refresh-interval

Sets the maximum number of seconds a device waits between sending updated Link State PDUs (LSPs) to its Intermediate System-to-Intermediate System (IS-IS) neighbors.

## Syntax

```
lsp-refresh-interval interval
```

```
lsp-refresh-interval interval
```

## Command Default

The default interval is 900 seconds (15 minutes).

## Parameters

*secs*

Specifies the interval in seconds. Valid values range from 1 through 65535 seconds. The default is 900 seconds.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command removes the configured interval.

## Examples

The following example changes the LSP refresh interval to 20000 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-refresh-interval 20000
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# lsr-id

Configures an IP address to be used as the LSR ID for the LDP identifier.

## Syntax

```
lsr-id ip_addr
```

```
no lsr-id ip_addr
```

## Command Default

The LSR-ID is the first available loopback interface address.

## Parameters

*ip\_addr*

Specifies the IP address to assign to the LSR identifier.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

You can configure only an IPv4 address.

Use the **no** form of the command to reset the default behavior. When you enter the **no** form of the command and LDP protocol is in the enabled state, the device uses the same LSR-ID until the LDP protocol is disabled; the IP address selected as LSR-ID for the LDP protocol is still valid and is the operationally UP IP address on an enabled loopback interface.

When you enter the **no** form of the command and LDP protocol is in the disabled state (this happens when the loopback interface on which IP address is configured is in the disabled state), the device falls back to default behavior which tries to enable LDP protocol when it finds a valid IP address on any one of the enabled loopback interfaces.

## Examples

The following example configures an IP address for the LSR identifier.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# lsr-id 10.22.22.22
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## mac access-group

Applies rules specified in a MAC access control list (ACL) to traffic entering or exiting an interface.

### Syntax

```
mac access-group ACLname { in | out }
```

```
no mac access-group ACLname { in | out }
```

### Parameters

*ACLname*

Specifies the name of the standard or extended MAC access list.

**in**

Applies the ACL to incoming switched and routed traffic.

**out**

Applies the ACL to outgoing routed traffic.

### Modes

Interface-subtype configuration mode

### Usage Guidelines

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces. And you can apply an ACL twice—ingress and egress—to a given user interface.

To remove an ACL from an interface, enter the **no** form of this command.

### Examples

The following example applies a MAC ACL to filter inbound packets only, on a specified Ethernet interface.

```
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# mac access-group macacl2 in
```

The following example removes a MAC ACL from a specified port-channel interface.

```
device(config)# interface port-channel 62
device(config-Port-channel-62)# no mac access-group macacl2 in
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mac access-list extended

Creates an extended MAC access control list (ACL). An extended ACL contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters.

## Syntax

```
mac access-list extended ACLname  
no mac access-list extended ACLname
```

## Parameters

*ACLname*

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

## Modes

Global configuration mode

## Usage Guidelines

Use this command to create an extended MAC access list. If the ACL is already created, this command puts the device in the extended MAC access-list configuration mode.

Extended ACLs allow you to filter traffic based on the following:

- Source MAC address
- Destination MAC address
- EtherType

You can apply named MAC extended ACLs to VLANs and to Layer 2 interfaces.

Standard and extended MAC ACLs cannot share the same name.

To remove a MAC ACL from an interface, enter the **no** form of this command.

## Examples

The following example creates a MAC extended ACL named mac1.

```
device(config)# mac access-list extended mac1  
device(conf-macl-ext)#
```

The following example deletes a MAC extended ACL named mac1.

```
device(conf-macl-ext)# no mac access-list extended mac1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mac access-list standard

Creates a standard MAC access control list (ACL). Standard ACLs contain rules that permit or deny traffic based on source addresses that you specify.

## Syntax

```
mac access-list standard ACLname
no mac access-list standard ACLname
```

## Parameters

*ACLname*

Specifies a unique ACL name. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

## Modes

Global configuration mode

## Usage Guidelines

Use this command to create a standard MAC access list. If ACL is already created, this command puts the device in the standard MAC access-list configuration mode.

Standard and extended MAC ACLs cannot share the same name.

To remove a MAC ACL from an interface, enter the **no** form of this command.

## Examples

The following command creates a MAC standard ACL named mac1.

```
device(config)# mac access-list standard mac1
device(conf-macl-std) #
```

The following command deletes a MAC standard ACL named mac1.

```
device(conf-macl-std) # no mac access-list standard mac1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# master-vlan (STP)

Selects a master VLAN for a topology group.

## Syntax

```
master-vlan vlan_id
```

## Command Default

The master VLAN is not configured.

## Parameters

*vlan\_id*

The master VLAN ID.

## Modes

Topology group configuration mode.

## Usage Guidelines

To configure a master VLAN, the VLAN must already be configured. The master VLAN contains the STP settings for all the VLANs in the STP per VLAN group. An STP group can have only one master VLAN. If you add a new master VLAN to an STP group that already has a master VLAN, the new master VLAN replaces the older master VLAN.

If you remove the master VLAN (by entering the **no master-vlan** command), the software selects the new master VLAN from member VLANs. A new candidate master VLAN will be in configured as a member VLAN so that the first added member VLAN will be a new candidate master VLAN. Once you save and reload, a member VLAN with the youngest VLAN ID will be the new candidate master.

## Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# match (route map)

Defines a variety of match conditions for a route map.

## Syntax

```

match as-path name
match community name exact-match ]
match extcommunity number
match interface { ethernet slot / port | loopback num | ve-interface vlan_id }
match ip address { acl name [ prefix-list string ] | prefix-list string [ acl name ] }
match ip next-hop prefix-list string
match ip route-source prefix-list string
match ipv6 next-hop prefix-list string
match ipv6 route-source prefix-list string
match metric num
match protocol bgp { external | internal | static-network }
match protocol static
match route-type { internal | type-1 | type-2 }
match tag num
match vrf name
no match as-path
no match community
no match extcommunity
no match interface
no match ip address
no match ip next-hop
no match ip route-source
no match ipv6 address
no match ipv6 next-hop
no match ipv6 route-source
no match metric
no match protocol
no match route-type
no match tag

```



## Command Default

This option is disabled.

## Parameters

### *as-path*

Matches an AS-path access list name in a route-map instance.

#### *name*

Name of an AS-path access list. Range is from 1 through 32 ASCII characters.

### **community**

Matches a BGP community access list name in a route-map instance.

#### *name*

Name of a BGP community access list. Values range from 1 through 32 ASCII characters.

#### **exact-match**

Matches a route only if the route community attributes field contains the same community numbers specified in the **match** statement.

### **extcommunity** *number*

Matches a BGP extended community list in a route-map instance and specifies an extended community list number. Valid values range from 1 through 99.

### **interface**

Matches interface conditions in a route-map instance.

### **ethernet**

Specifies an ethernet interface.

#### *slot*

Specifies a valid slot number.

#### *port*

Specifies a valid port number.

### **loopback** *num*

Specifies a loopback interface.

### **ve-interface** *vlan\_id*

Specifies a virtual Ethernet VLAN interface.

### **ip address**

Matches an IP address in a route-map instance.

#### **acl** *name*

Name of the access list. Range is from 1 through 32 ASCII characters.

#### **prefix-list** *string*

Specifies an IP prefix list. Range is from 1 through 32 ASCII characters.

### **ip next-hop**

Matches IP next-hop match conditions in a route-map instance.

### **ip route-source**

Matches an IP route source in a route-map instance.

**ipv6 address**

Matches an IPv6 address in a route-map instance.

**ipv6 next-hop**

Matches IPv6 next-hop match conditions in a route-map instance.

**ipv6 route-source**

Matches an IPv6 route source in a route-map instance.

**metric *num***

Matches a route metric in a route-map instance. Values range from 0 through 4294967295.

**protocol bgp external**

Matches on BGP routes.

**protocol bgp internal**

Matches on iBGP routes.

**protocol bgp static-network**

Matches on BGP4 static network routes. This is applicable only for BGP outbound policy.

**protocol static**

Matches on static routes.

**route-type**

Matches a route type in a route-map instance.

**internal**

Internal route type

**type-1**

OSPF external route type 1

**type-2**

OSPF external route type 2

**tag *tag-value***

Specifies a route tag and route tag value.

**vrf *name***

Specifies a non-default VRF. Valid values range from 0 through 4294967295.

## Modes

Route-map configuration mode

## Usage Guidelines

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

## Examples

The following example matches AS-path ACL 1 in route-map instance "myroutes".

```
device#configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map myroutes/permit/10)# match as-path 1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# match access-group

Matches an ACL to a class map.

## Syntax

```
match access-group name
```

## Parameters

*name*

The ACL name.

## Modes

Class map configuration mode.

## Usage Guidelines

class-map

## Examples

Use this command to match an ACL to a class map.

```
device(config)# class-map default  
device(config-classmap)# match access-group class_acl
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# maxas-limit

Imposes a limit on the number of autonomous systems in the AS-PATH attribute.

## Syntax

`maxas-limit in num`

`no maxas-limit in`

## Command Default

Disabled.

## Parameters

*in*

Allows an AS-PATH attribute from any neighbor to impose a limit on the number of autonomous systems.

*num*

Range is from 0 through 300. The default is 300.

## Modes

BGP configuration mode

## Usage Guidelines

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

## Examples

This example sets the limit on the number of BGP4 autonomous systems in the AS-PATH attribute to 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maxas-limit in 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# maximum-paths (BGP)

Sets the maximum number of BGP4 and BGP4+ shared paths.

## Syntax

```
maximum-paths num | use-load-sharing
no maximum-paths
```

## Command Default

Disabled.

## Parameters

*num*

Specifies the maximum number of paths across which the device balances traffic to a given BGP destination. Valid values range is from 1 through 64. The default is 1.

**use-load-sharing**

Uses the maximum IP ECMP path value supported (64) without enabling BGP level ECMP.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use this command to change the maximum number of BGP4 shared paths, either by setting a value or using the maximum IP ECMP path value supported (64) without enabling BGP level ECMP.

If the configured *num* value is less than the possible number of ECMP paths available, BGP routes may not take the same number of ECMP paths. The set of ECMP paths may not be the same for different prefixes.

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

## Examples

This example sets the maximum number of BGP4 shared paths to 8.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maximum-paths 8
```

This example sets the maximum number of BGP4+ shared paths to 64 without enabling BGP level ECMP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths use-load-sharing
```

This example sets the maximum number of BGP shared paths to 2 in a nondefault VRF instance in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# maximum-paths 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# maximum-paths (IS-IS)

Specifies the number of paths Intermediate System-to-Intermediate System (IS-IS) can calculate and install in the IPv4 or IPv6 forwarding table.

## Syntax

`maximum-paths number`

`no maximum-paths number`

## Command Default

The default is 8 paths.

## Parameters

*value*

Specifies the number of paths. Valid values range from 1 through 64 paths. The default is 8.

## Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

## Usage Guidelines

The **no** form of the command resets number of paths to the default number of 8.

## Examples

The following example specifies that the number of paths IS-IS can calculate and install in the IP forwarding table is 10.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# maximum-paths 10
```

The following example resets the number of paths IS-IS can calculate and install in the IPv6 forwarding table to 8 (the default).

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# maximum-paths (OSPF)

Changes the maximum number of OSPF shared paths.

## Syntax

**maximum-paths** *num*

**no maximum-paths**

## Command Default

This option is disabled.

## Parameters

*num*

Maximum number of paths across which the device balances traffic to a given OSPF destination. The range is from 1 through 64. The default is 8.

## Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

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

## Examples

The following example sets the maximum number of shared paths to 22.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# maximum-paths 22
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# maximum-paths ebgp ibgp

Specifies the number of equal-cost multipath eBGP or iBGP routes or paths that are selected.

## Syntax

```
maximum-paths { ebgp num | ibgp num }  
no maximum-paths
```

## Command Default

This option is disabled.

## Parameters

<b>ebgp</b>	Specifies eBGP routes or paths.
<b>ibgp</b>	Specifies iBGP routes or paths.
<i>num</i>	The number of equal-cost multipath routes or paths that are selected. Range is from 1 through 64. 1 disables equal-cost multipath.

## Modes

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

## Usage Guidelines

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

Enhancements to BGP load sharing support the load sharing of BGP4 and BGP4+ routes in IP Equal-Cost Multipath (ECMP), even if the BGP multipath load-sharing feature is not enabled by means of the **use-load-sharing** option for the **maximum-paths** command. You can set separate values for IGMP and ECMP load sharing. Use this command to specify the number of equal-cost multipath eBGP or iBGP routes or paths that are selected.

## Examples

This example sets the number of equal-cost multipath eBGP routes or paths that will be selected to 6 in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maximum-paths ebgp 6
```

This example sets the number of equal-cost multipath iBGP routes or paths that will be selected to 4 in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths ibgp 4
```

This example sets the number of equal-cost multipath EBGP routes or paths that will be selected to 3 for the IPv4 address family for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# maximum-paths ebgp 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# max-age

Sets the interval time in seconds between messages that the spanning tree receives from the interface.

## Syntax

**max-age** *seconds*

**no max-age**

## Command Default

20 seconds.

## Parameters

*seconds*

Configures the STP interface maximum age. Valid values range from 6 through 40.

## Modes

Spanning tree configuration mode

## Usage Guidelines

Use this command to control the maximum length of time that passes before an interface saves its configuration Bridge Protocol Data Unit (BPDU) information.

If the **vlan** parameter is not provided, the *seconds* value is applied globally for all per-VLAN instances. However, for VLANs that have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

When configuring the maximum age, the **max-age** command setting must be greater than the **hello-time** command setting. The following relationship should be kept:

$$(2 \times (\text{forward-delay} - 1)) \geq \text{max-age} \geq (2 \times (\text{hello-time} + 1))$$

Enter **no max-age** to return to the default configuration.

## Examples

To configure the maximum age to 10 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# max-age 10
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# max-age 10
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# max-age 10
```

```
device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# max-age 10
```

```
device# configure terminal
device(config)# protocol spanning-tree rpvt
device(conf-rpvt)# max-age 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# max-lsp-lifetime

Sets the maximum number of seconds an unrefreshed Link State PDU (LSP) remains in the LSP database of a device.

## Syntax

**max-lsp-lifetime** *secs*

**max-lsp-lifetime** *secs*

## Command Default

The default maximum lifetime is 1200 seconds (20 minutes).

## Parameters

*secs*

Specifies the maximum lifetime in seconds. Valid values range from 1 through 65535 seconds. The default is 1200 seconds.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **max-lsp-lifetime** and **lsp-refresh-interval** commands must be configured in such a way that the LSPs are refreshed before the maximum LSP lifetime is reached; otherwise, the device's originated LSPs may be timed out by neighbors of the device.

The **no** form of the command removes the configured period of time.

## Examples

The following example changes the maximum LSP lifetime to 2400 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# max-lsp-lifetime 2400
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# max-mcache

Configures the maximum multicast cache size.

## Syntax

**max-mcache** *num*

**no max-mcache**

## Command Default

Multicast cache size is 24576 entries.

## Parameters

*num*

Number of entries in the multicast cache. Valid values range from 1 through 24576.

## Modes

Router PIM configuration mode

## Usage Guidelines

Entering the **no** form of the command sets the maximum multicast cache size to the default - 24576 entries.

## Examples

Setting the multicast cache to 500 entries.

```
device(config)# router pim
device(conf-pim-router)# max-mcache 500
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# max-metric router-lsa

Advertises the maximum metric value in different Link State Advertisements (LSAs).

## Syntax

```
max-metric router-lsa [ all-vrfs ] [ all-lsas | external-lsa metric-value | link { all | ptp | stub | transit } | summary-lsa metric-value | on-startup { time | wait-for-bgp [ all-lsas | summary-lsa metric-value | external-lsa metric-value | link { all | ptp | stub | transit } ] }
```

```
max-metric router-lsa [ all-vrfs ] [ all-lsas | external-lsa | link { all | ptp | stub | transit } | summary-lsa | on-startup { time | wait-for-bgp [ all-lsas | summary-lsa | external-lsa | link { all | ptp | stub | transit } ] }
```

## Parameters

### all-vrfs

Applies the configuration change to all instances of OSPF.

### all-lsas

Sets the **summary-lsa** and **external-lsa** optional parameters to the corresponding default max-metric value. For a non-default instance of OSPF, only the summary-lsa and external-lsa parameters are set.

### external-lsa *metric-value*

Modifies the metric of all external type 5 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFE), and the default is 16711680 (0x00FF0000).

### link

Specifies the types of links for which the maximum metric is advertised. By default, the maximum metric is advertised only for transit links.

#### all

Advertises the maximum metric in Router LSAs for all supported link types.

#### ptp

Advertises the maximum metric in Router LSAs for point-to-point links.

#### stub

Advertises the maximum metric in Router LSAs for stub links.

#### transit

Advertises the maximum metric in Router LSAs for transit links. This is the default link type.

### summary-lsa *metric-value*

Modifies the metric of all summary type 3 and type 4 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777215 (0x00001 - 0x00FFFFE), and the default is 16711680 (0x00FF0000).

### on-startup

Applies the configuration change at the next OSPF startup.

#### *time*

Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86,400.



**wait-for-bgp**

Indicates that OSPF should wait for either 600 seconds or until BGP has finished route table convergence, whichever happens first, before advertising the links with the normal metric.

## Modes

OSPF router configuration mode

OSPF VRF router configuration mode

## Usage Guidelines

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

Enter **no max-metric router-lsa all-lsas** to disable advertising the maximum metric value in different LSAs.

## Examples

The following example advertises the maximum metric value using the **all-lsas** option.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# max-metric router-lsa all-lsas
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# max-metric router-lsa (OSPFv3)

Advertises the maximum metric value in different Link State Advertisements (LSAs).

## Syntax

```
max-metric router-lsa [ all-lsas | external-lsa metric-value | include-stub | on-startup { time | wait-for-bgp } | summary-lsa metric-value ]
```

```
no max-metric router-lsa [ all-lsas | external-lsa | include-stub | on-startup { time | wait-for-bgp } | summary-lsa ]
```

## Parameters

### all-lsas

Sets the **summary-lsa** and **external-lsa** optional parameters to the corresponding default max-metric value. For a non-default instance of OSPFv3, only the summary-lsa and external-lsa parameters are set.

### external-lsa *metric-value*

Configures the maximum metric value for all external type-5 and type-7 LSAs. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFFE), and the default is 16711680 (0x00FF0000).

### include-stub

Specifies the advertisement of the maximum metric value for point-to-point and broadcast stub links in the intra-area-prefix LSA..

### on-startup

Applies the configuration change at the next OSPF startup.

#### *time*

Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86400.

### wait-for-bgp

Specifies that OSPFv3 should wait until BGP has finished route table convergence before advertising the links with the normal metric, or for no more than 600 seconds.

### summary-lsa *metric-value*

Configures the maximum metric value for all summary type 3 and type 4 LSAs. The range for metric value is 1 to 16777215 (0x00001 - 0x00FFFFFFE), and the default is 16711680 (0x00FF0000).

## Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

## Usage Guidelines

Enter **no max-metric router-lsa** to disable advertising the maximum metric value in different LSAs.

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the

route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

## Examples

This example configures an OSPFv3 device to advertise a maximum metric and sets the maximum metric value for all external type-5 and type-7 LSAs to 1000.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa external-lsa 1000
```

This example configures an OSPFv3 device to advertise a maximum metric and specifies the advertisement of the maximum metric value for point-to-point and broadcast stub links in the intra-area-prefix LSA.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa include-stub
```

This example configures an OSPFv3 device to advertise a maximum metric until BGP routing tables converge or until the default timer of 600 seconds expires.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa on-startup wait-for-bgp
```

This example configures an OSPFv3 device to advertise a maximum metric and sets the maximum metric value for all summary type-3 and type-4 LSAs to 100.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa summary-lsa 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# max-neighbor-reconnect-time

Specifies the maximum time that this router must wait for a graceful restart (GR) neighbor to restore the LDP session.

## Syntax

**max-neighbor-reconnect-time** *seconds*

**no max-neighbor-reconnect-time** *seconds*

## Command Default

120 seconds

## Parameters

*seconds*

Specifies the maximum time in seconds that this router must wait for a GR neighbor to restore the LDP session. Enter a integer from 60 to 300. The default setting is 120.

## Modes

MPLS LDP GR configuration mode

## Usage Guidelines

The **no** form of the command resets the default time of 120 seconds.

## Examples

The following example sets the LDP GR timer to 180 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# max-neighbor-reconnect-time 180
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# max-neighbor-recovery-time

Specifies the maximum amount of time that this router waits for a graceful restart (GR) neighbor to complete its GR recovery after the LDP session has been reestablished.

## Syntax

```
max-neighbor-recovery-time seconds
no max-neighbor-recovery-time seconds
```

## Command Default

The default maximum time is 120 seconds.

## Parameters

*seconds*

Specifies the maximum amount of time in seconds that this router waits for a GR neighbor to complete its GR recovery after the LDP session has been reestablished. Enter an integer from 60 to 3600. The default setting is 120.

## Modes

MPLS LDP GR configuration mode

## Usage Guidelines

Recovery-time must be chosen accordingly taking into account the time it takes for RTM to recompute the routes and the number of Layer 3 FECs that need to be recovered as part of the LDP GR recovery. This is applicable to GR processing on ingress as well as transit LSRs.

The **no** form of the command resets the default time of 120 seconds.

## Examples

The following example sets the LDP GR timer to 240 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# max-neighbor-recovery-time 240
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# med-missing-as-worst

Configures the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

## Syntax

```
med-missing-as-worst
no med-missing-as-worst
```

## Command Default

This option is disabled.

## Modes

BGP configuration mode

## Usage Guidelines

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

When MEDs are compared, by default the device favors a low MED over a higher one. Because the device assigns a value of 0 to a route path MED if the MED value is missing, the default MED comparison results in the device favoring the route paths that do not have MEDs.

## Examples

This example configures the device to favor a route containing a MED.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# med-missing-as-worst
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# member-bridge-domain

Configures member bridge domains for a topology group.

## Syntax

```
member-bridge-domain { add | remove } bridge_domain_id
```

## Command Default

The topology group has no member bridge domains.

## Parameters

### add

Add a bridge domain to the topology group.

### remove

Remove a bridge domain from the topology group.

### bridge\_domain\_id

Bridge domain ID or the bridge domain range; for example: 1, 2, 4-7, 8, 9-22, 55-66. The maximum is 253 characters.

## Modes

Topology group configuration mode.

## Usage Guidelines

You must first add a master VLAN to the topology group.

## Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
device(config-topo-group-10)# member-bridge-domain add 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# member vlan

Adds VLANs as members to the MCT cluster.

## Syntax

```
member vlan { add | remove } member-vlan
no member
```

## Parameters

### add

Adds a VLAN or a range of VLANs to the MCT cluster.

### remove

Removes configured member VLANs from the MCT cluster.

### *member-vlan*

Specifies the VLAN members of the MCT cluster. You can include an individual VLAN and a range of VLANs. To specify a range of VLAN, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual and ranges of VLANs, separate them by commas (for example, 1,2,4-7,8,9-22,55-66). You can enter a maximum of 253 characters.

## Modes

Cluster configuration mode

## Usage Guidelines

The member VLAN group must be configured before deploying the cluster.

Each cluster can control up to 4096 VLANs. The VLANs within a VLAN group have the same ports and use the same values for other VLAN parameters.

The **no** form of the command removes all member VLANs from the MCT cluster.

## Examples

The following example adds the VLAN members to the MCT cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# member vlan add 2,4-7
```

The following example removed VLAN members from the MCT cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# member vlan remove 4-7
```



# History

Release version	Command history
16r.1.01	This command was introduced.

# member-vlan (STP)

Adds member VLANs to an STP topology group.

## Syntax

```
member-vlan { add | remove } vlan_id
```

## Command Default

The topology group has no member VLANs.

## Parameters

### add

Add a VLAN to the topology group.

### remove

Remove a VLAN from the topology group.

### vlan\_id

Adds a member VLAN ID to the STP topology group. This can be a single VLAN or a range of VLANs. For example: 2, 4-7, 8, 9-22, 55-66. The maximum input is 253 characters.

## Modes

Topology group configuration mode.

## Usage Guidelines

The VLAN(s) must be configured before adding to the topology group.

You must first add a master VLAN to the topology group.

All the VLANs in the member group inherit the STP settings of the master VLAN in the group.

## Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
device(config-topo-group-10)# member-vlan add 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# message-interval

Configures the Protocol Independent Multicast (PIM) Join or Prune message interval.

## Syntax

```
message-interval num
no message-interval num
```

## Command Default

60 seconds

## Parameters

*num*

The interval value in seconds. Valid values range from 10 through 65535 seconds.

## Modes

Router PIM configuration mode

## Usage Guidelines

Use this command to specify the interval at which the periodic PIM Join or Prune messages must be sent out.

Enter the **no** form of the command to disable this feature.

## Examples

Setting the interval to one hour.

```
device(config)# router pim
device(conf-pim-router)# message-interval 3600
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## metric

Assigns a metric to the LSP, which routing protocols can use to determine the relative preference among several LSPs towards a given destination.

## Syntax

**metric** *number*

**no metric** *number*

## Command Default

All LSPs have a metric of 1.

## Parameters

*number*

Specifies the metric value. Enter an integer from 1 to 65535. A lower value is preferred over a higher value.

## Modes

MPLS LSP configuration mode

## Usage Guidelines

When multiple LSPs have the same destination LSR, and they have the same metric, the traffic load is shared among them.

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

## Examples

The following example configures LSP to22 with a metric value of 20.

```
device(config)# router mpls
device(config-router-mpls)# lsp to22
device(config-router-mpls-lsp-to22)# no enable
device(config-router-mpls-lsp-to22)# to 10.1.1.2
device(config-router-mpls-lsp-to22)# from 10.1.1.1
device(config-router-mpls-lsp-to22)# metric 20
device(config-router-mpls-lsp-to22)# enable
device(config-router-mpls-lsp-to22)#exit
```

## History

Release	Command history
16r. 1.00	This command is introduced.

# metric-style wide

Enables the wide metric type for new style of TLVs with Intermediate System-to-Intermediate System (IS-IS).

## Syntax

```
metric-style wide [ level-1 | level-2 ]
```

```
no metric-style wide
```

## Command Default

The wide metric type is not used.

## Parameters

### level-1

Specifies the IS-IS routing parameter as Level 1.

### level-2

Specifies the IS-IS routing parameter as Level 2.

## Modes

IS-IS address-family IPv4 unicast configuration mode

## Usage Guidelines

When LDP-IGP synchronization is enabled, the wide metric type must be used.

The **no** form of the command disables the use of the wide metric type.

## Examples

The following example enables the wide metric type for Level 1 packets for the IS-IS IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# metric-style wide level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# metric-type

Configures the default metric type for external routes.

## Syntax

```
metric-type { type1 | type2 }
no metric-type { type1 | type2 }
```

## Command Default

Type 1

## Parameters

### type1

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

### type2

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

## Modes

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

## Usage Guidelines

The **no** form of the command restores the default setting. You must specify a type parameter when using the **no** form.

## Examples

The following example sets the default metric type for external routes to type 2.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# metric-type type2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mode gre ip

Enables generic routing encapsulation (GRE) over a tunnel interface and specifies that the tunneling protocol is IPv4.

## Syntax

```
mode gre ip
no mode
```

## Command Default

GRE is disabled.

## Modes

Interface tunnel configuration mode

## Usage Guidelines

Use the **no mode gre ip** command to disable the GRE IP tunnel encapsulation method for the tunnel interface.

## Examples

This example enables GRE IP encapsulation on a tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mode (LLDP)

Sets the LLDP mode on the device.

## Syntax

```
mode { tx | rx }
```

## Command Default

Both transmit and receive modes are enabled.

## Parameters

- tx**  
Specifies to enable only the transmit mode.
- rx**  
Specifies to enable only the receive mode.

## Modes

Protocol LLDP configuration mode

## Examples

To enable only the transmit mode:

```
device(conf-lldp)# mode tx
```

To enable only the receive mode:

```
device(conf-lldp)# mode rx
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# mode (port-group)

Configures the ports in a port group of an SLX 9850 36x100G line card as 40G and activates all 10 ports.

## Syntax

```
mode { 40g | 100g }
```

## Command Default

The six ports of a 36X100G port group are configured as 100G and the remaining four are inactive.

## Parameters

**40g**

Configures the ports in a port group as 40G and activates all 10 ports.

**100g**

Configures the default setting of six ports in the port group as 100G and the remaining four ports are inactive.

## Modes

Hardware port-group configuration mode

## Usage Guidelines

Before changing the port speed, you must power off the line card.

You can configure more than one port group on a LC before restoring its power.

## Examples

The following example shows the configuration of the ports in a port group as 40G and all 10 ports are activated.

```
device# power-off linecard 3
device# configure terminal
device(config)# hardware
device(config-hardware)# port-group 3/1
device(config-port-group-3/1)# mode 40g
%Warning: port-group mode is a disruptive command.
Please power-cycle the line-card for the changes to take place
device(config-port-group-3/1)# Ctrl-z
device# power-on linecard 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mpls-interface

Configures MPLS on an interface and accesses MPLS interface subconfiguration mode to configure its parameters.

## Syntax

```
mpls-interface { ethernet slot/port | ve number}
no mpls-interface { ethernet slot/port | ve number}
```

## Command Default

None

## Parameters

**ethernet slot/port**  
Specifies an Ethernet slot and port.

**ve number**  
Specifies the VE interface number.

## Modes

MPLS configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the MPLS interface.

You cannot configure MPLS on a VE interface associated with a protocol based VLAN. The command is rejected, and an error message is displayed.

After you enable MPLS globally on the device, you can enable it on one or more interfaces.

## Examples

The following example configures MPLS on Ethernet interface 1/12.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/12
device(config-router-mpls-interface-1/12)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mpls reoptimize

Under ordinary conditions, an LSP path does not change unless the path becomes inoperable. Consequently, the router must be directed to consider configuration changes made to an LSP and to optimize the LSP path based on those changes.

## Syntax

```
mpls reoptimize { all | lsp lsp_name }
```

## Command Default

None.

## Parameters

**all**

Reoptimizes all LSPs.

**lsp***lsp\_name*

Reoptimizes the specified LSP.

## Modes

Privileged EXEC mode.

## Usage Guidelines

On re-optimization of an adaptive LSP, LSP accounting statistics might miss the accounting of some of the packets.

## Examples

The following example uses the **mpls re-optimize** command to re-optimize LSP *to20*.

```
device# mpls reoptimize lsp to20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mtu

Configures the maximum transmission unit (MTU) for a pseudowire (PW) profile.

## Syntax

**mtu** *mtu-value*

**no mtu**

## Command Default

The MTU value is set to 1500.

## Parameters

*mtu-value*

Specifies the maximum transmission unit (MTU) for the PW profile. Values range from 64 through 15966.

## Modes

Pseudowire-profile configuration mode.

## Usage Guidelines

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

## Examples

The following example shows how to set the MTU value to 2000 for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# mtu 2000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# mtu-enforce

Configures MTU enforcement check for a pseudowire (PW) profile.

## Syntax

```
mtu-enforce { false | true }
no mtu-enforce
```

## Command Default

MTU enforcement is disabled.

## Parameters

*false*  
Disables the MTU enforcement check.

*true*  
Enables the MTU enforcement check.

## Modes

Pseudowire-profile configuration mode.

## Usage Guidelines

MTU enforcement is only supported during PW signaling.

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

## Examples

The following example shows how to enable MTU enforcement check for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# mtu-enforce true
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# multipath

Changes load sharing to apply to only iBGP or eBGP paths, or to support load sharing among paths from different neighboring autonomous systems.

## Syntax

```
multipath { ebgp | ibgp | multi-as }  
no multipath { ebgp | ibgp | multi-as }
```

## Command Default

This option is disabled.

## Parameters

- ebgp**  
Enables load sharing of eBGP paths only.
- ibgp**  
Enables load sharing of iBGP paths only.
- multi-as**  
Enables load sharing of paths from different neighboring autonomous systems.

## Modes

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

## Usage Guidelines

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

By default, when BGP load sharing is enabled, both iBGP and eBGP paths are eligible for load sharing, while paths from different neighboring autonomous systems are not.

## Examples

This example changes load sharing to apply to iBGP paths in the IPv4 address family.

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

This example enables load sharing of paths from different neighboring autonomous systems in the IPv6 address family.

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

This example changes load sharing to apply to eBGP paths in IPv4 VRF instance "red":

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# multiplier (LLDP)

Sets the number of consecutive misses of hello messages before LLDP declares the neighbor as dead.

## Syntax

`multiplier value`

`no multiplier`

## Command Default

Multiplier default value is 4.

## Parameters

*value*

Specifies a multiplier value to use. Valid values range from 2 through 10.

## Modes

Protocol LLDP and profile configuration modes

## Usage Guidelines

Enter `no multiplier` to return to the default setting.

The LLDP multiplier can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the `lldp profile` command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

## Examples

To set the number of consecutive misses:

```
device(config-lldp)# multiplier 2
```

To set the number of consecutive misses for a specific LLDP profile:

```
device(config-lldp)# profile test1
device(config-profile-test1)# multiplier 5
device(config-profile-test1)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# multiplier (UDLD)

Sets timeout multiplier for missed UDLD PDUs.

## Syntax

`multiplier value`

`no multiplier`

## Command Default

Multiplier default value is 5.

## Parameters

*value*

Specifies a multiplier value to use. Valid values range from 3 through 10.

## Modes

Protocol UDLD configuration mode

## Usage Guidelines

When the device at one end is an Extreme Networks IP product, the timeout interval is the product of the "hello" time interval at the other end and the "multiplier" value.

When the UDLD protocol times out waiting for UDLD PDUs, it will block the port.

Enter **no multiplier** to return to the default setting.

## Examples

To set the multiplier to 8:

```
device# configure terminal
device(config)# protocol udld
device(config-udld)# multiplier 8
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# multi-topology

Enables IPv6 Intermediate System-to-Intermediate System (IS-IS) MT in an area or a domain so that the MT-enabled device runs IPv6 IS-IS in multi SPF mode.

## Syntax

```
multi-topology [ transition ]  
no multi-topology [ transition ]
```

## Command Default

The transition option is disabled.

## Parameters

### transition

Enables IPv6 IS-IS MT transition mode in an area or a domain so that a network operating in IPv6 IS-IS single-topology support mode can continue to work while upgrading devices to include IPv6 IS-IS MT support.

## Modes

IS-IS address-family IPv6 unicast configuration mode

## Usage Guidelines

When transition mode is not enabled, the routers operating in single-topology mode do not establish IPv6 connectivity with the routers operating in MT mode.

The **no** form of the command disables IPv6 IS-IS MT.

## Examples

The following example enables IPv6 IS-IS MT.

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

The following example enables IPv6 IS-IS MT with transition support.

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

## History

Release version	Command history
16r.1.00	This command was introduced.



# Commands N - Q

---

## nbr-timeout

Configures the neighbor timeout interval after which a neighbor is considered to be absent.

### Syntax

```
nbr-timeout num
```

```
no nbr-timeout
```

### Command Default

The default is 105 seconds.

### Parameters

*num*

Interval value in seconds. Valid values range from 35 through 12600 seconds.

### Modes

Router PIM configuration mode

### Usage Guidelines

Neighbor timeout is the interval after which a PIM device will consider a neighbor to be absent. Absence of PIM hello messages from a neighboring device indicates that a neighbor is not present. The interval can be set between 3 and 65535 seconds, and it should not be less than 3.5 times the hello timer value.

Enter **no nbr-timeout** to disable this feature.

### Examples

Setting the timeout to 600 seconds.

```
device(config)# router pim
device(config-pim-router)# nbr-timeout 600
```

### History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor activate

Enables the exchange of information with BGP neighbors and peer groups.

## Syntax

**neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

**no neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

## Command Default

Enabling address exchange for the IPv4 address family is enabled. Enabling address exchange for the IPv6 address family is disabled.

## Parameters

*ip-address*

Specifies the IPv4 address of the neighbor.

*ipv6-address*

Specifies the IPv6 address of the neighbor.

*peer-group-name*

Specifies a peer group.

## Modes

BGP address-family EVPN configuration mode

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to disable the exchange of an address with a BGP neighbor or peer group.

## Examples

This example establishes a BGP session with a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 activate
```

This example establishes a BGP EVPN session with a neighbor with the IP address 10.1.1.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 activate
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor advertisement-interval

Enables changes to the interval over which a specified neighbor or peer group holds route updates before forwarding them.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } advertisement-interval seconds
no neighbor { ip-address | ipv6-address | peer-group-name } advertisement-interval
```

## Command Default

The default is 0.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*seconds*

Range is from 0 through 3600.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Examples

This example changes the BGP4 advertisement interval from the default to 60 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 advertisement-interval 60
```

This example changes the BGP4+ advertisement interval from the default for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 advertisement-interval 60
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor allowas-in

Disables the AS\_PATH check function for routes learned from a specified neighbor so that BGP does not reject routes that contain the recipient BGP speaker's AS number.

## Syntax

```
neighbor {ip-address | ipv6-address | peer-group-name } allowas-in number
no neighbor allowas-in {ip-address | ipv6-address | peer-group-name } allowas-in
```

## Command Default

The AS\_PATH check function is enabled and any route whose path contains the speaker's AS number is rejected as a loop.

## Parameters

*ip-address*

Specifies the IP address of the neighbor.

*ipv6-address*

Specifies the IPv6 address of the neighbor.

*peer-group-name*

Specifies a peer group.

*number*

Specifies the number of times that the AS path of a received route may contain the recipient BGP speaker's AS number and still be accepted. Valid values are 1 through 10.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

The **no** form of the command re-enables the AS\_PATH check function.

If the AS\_PATH check function is disabled after a BGP session has been established, the neighbor session must be cleared for this change to take effect.

## Examples

The following example specifies that the AS path of a received route may contain the recipient BGP4+ speaker's AS number three times and still be accepted.

```
device#configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example specifies for VRF instance "red" that the BGP4+ AS path of a received route may contain the recipient BGP speaker's AS number three times and still be accepted.

```
device#configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::124 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor as-override

Replaces the autonomous system number (ASN) of the originating device with the ASN of the sending BGP device.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } as-override
```

```
no neighbor { ip-address | ipv6-address | peer-group-name } as-override
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the `neighbor peer-group-name` command.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

BGP loop prevention verifies the ASN in the AS path. If the receiving router sees its own ASN in the AS path of the received BGP packet, the packet is dropped. The receiving router assumes that the packet originated from its own AS and has reached the place of origination. This can be a significant problem if the same ASN is used among various sites, preventing sites with identical ASNs from being linked by another ASN. In this case, routing updates are dropped when another site receives them.

## Examples

This example replaces the ASN globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 as-override
```

This example replaces the BGP4+ ASN for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 as-override
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor capability as4

Enables or disables support for 4-byte autonomous system numbers (ASNs) at the neighbor or peer-group level.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } capability as4 [ disable | enable ]
```

```
no neighbor { ip-address | ipv6-address | peer-group-name } capability as4 [ disable | enable ]
```

## Command Default

4-byte ASNs are disabled by default.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor .

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

**disable**

Disables 4-byte numbering.

**enable**

Enables 4-byte numbering.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **disable** keyword or the **no** form of this command to remove all neighbor capability for 4-byte ASNs.

4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

## Examples

This example enables 4-byte ASNs for a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 capability as4 enable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor capability orf prefixlist

Advertises outbound route filter (ORF) capabilities to peer routers.

## Syntax

```
neighbor { ip_address | ipv6_address | peer-group-name } capability orf prefixlist [ receive | send ]
no neighbor { ip_address | ipv6_address | peer-group-name } capability orf prefixlist [ receive | send ]
```

## Command Default

ORF capabilities are not advertised to a peer device.

## Parameters

*ip\_address*

Specifies the IPv4 address of the neighbor.

*ipv6\_address*

Specifies the IPv6 address of the neighbor.

*peer-group-name*

Specifies a peer group.

**receive**

Enables the ORF prefix list capability in receive mode.

**send**

Enables the ORF prefix list capability in send mode.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to disable ORF capabilities.

## Examples

This example advertises the ORF send capability to a neighbor with the IP address 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 capability orf prefixlist send
```



This example advertises the ORF receive capability to a neighbor with the IPv6 address 2001:2018:8192::125 for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 capability orf prefixlist receive
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor default-originate

Configures the device to send the default route 0.0.0.0 to a neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } default-originate
no neighbor { ip-address | ipv6-address | peer-group-name } default-originate
```

## 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 unicast VRF configuration mode
- BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

The following example sends the default route to the BGP4 neighbor 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 default-originate
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor description

Specifies a name for a neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } description string  
no neighbor { ip-address | ipv6-address | peer-group-name } description
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

**description string**

Specifies the name of the neighbor, an alphanumeric string up to 220 characters long.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

This example specifies a BGP4 neighbor name.

```
device# configure terminal  
device(config)# router bgp  
device(config-bgp-router)# neighbor 10.11.12.13 description mygoodneighbor
```

This example specifies a BGP4+ neighbor name for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 default-originate route-map myroutemap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor ebgp-btsh

Enables BGP time to live (TTL) security hack protection (BTSH) for eBGP.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } ebgp-btsh
```

```
no neighbor { ip-address | ipv6-address | peer-group-name } ebgp-btsh
```

## Command Default

Disabled.

## Parameters

*ip-address*

Specifies the IPv4 address of the neighbor.

*ipv6-address*

Specifies the IPv6 address of the neighbor.

*peer-group-name*

Specifies a peer group.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

To maximize the effectiveness of this feature, the **neighbor ebgp-btsh** command should be executed on each participating device. The **neighbor ebgp-btsh** command is supported for both directly connected peering sessions and multihop eBGP peering sessions. For directly connected neighbors, when the **neighbor ebgp-btsh** command is used, the device expects BGP control packets received from the neighbor to have a TTL value of either 254 or 255. For multihop peers, when the **neighbor ebgp-btsh** command is used, the device expects the TTL for BGP control packets received from the neighbor to be greater than or equal to 255 minus the configured number of hops to the neighbor.

The **no** form of the command disables BTSH for eBGP.

## Examples

The following example enables GTSM between a device and a neighbor with the IP address 10.10.10.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.1.1.1 ebgp-btsh
```

The following example enables GTSM between a device and a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 ebgp-btsh
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor ebgp-multihop

Allows eBGP neighbors that are not on directly connected networks and sets an optional maximum hop count.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } ebgp-multihop [ max-hop-count ]
no neighbor { ip-address | ipv6-address | peer-group-name } ebgp-multihop
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*max-hop-count*

Maximum hop count (optional). Range is from 1 through 255.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

The **no** form of the command disables this feature.

## Examples

This example enables eBGP multihop and sets the maximum hop count to 20.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 ebgp-multihop 20
```



This example enables BGP4+ eBGP multihop for VRF instance "red" and sets the maximum hop count to 40.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 ebgp-multihop 40
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor enforce-first-as

Ensures that a device requires the first ASN listed in the AS\_SEQUENCE field of an AS path-update message from EBGP neighbors to be the ASN of the neighbor that sent the update.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } enforce-first-as [ disable | enable ]
no neighbor { ip-address | ipv6-address | peer-group-name } enforce-first-as [ disable | enable ]
```

## Command Default

Disabled by default.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor** *peer-group-name* command.

**disable**

Disables this feature.

**enable**

Enables this feature.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to disable this requirement globally for the device.

## Examples

This example enables the enforce-first-as feature for a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 enforce-first-as enable
```

This example enables the enforce-first-as feature for a BGP4+ specified neighbor for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 enforce-first-as enable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor filter-list

Specifies a filter list to be applied to updates from or to the specified neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } filter-list ip-prefix-list-name { in | out }
```

```
no neighbor { ip-address | ipv6-address | peer-group-name } filter-list ip-prefix-list-name { in | out }
```

## Command Default

No filter list is applied.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*ip-prefix-list-name*

Name of the filter list. The name must be between 1 and 63 ASCII characters in length.

**in**

Specifies that the list is applied on updates received from the neighbor.

**out**

Specifies that the list is applied on updates sent to the neighbor.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

This example specifies that filter list "myfilterlist" be applied to updates to a neighbor with the IP address 10.11.12.13 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 filter-list myfilterlist out
```

This example specifies that filter list "2" be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 filter-list 2 in
```

This example specifies that filter list "2" be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125 for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 filter-list 2 in
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor local-as

Causes the device to prepend the local autonomous system number (ASN) automatically to routes received from an eBGP peer.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } local-as num [ no-prepend ]
no neighbor { ip-address | ipv6-address | peer-group-name } local-as num [ no-prepend ]
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*num*

Local ASN. Range is from 1 through 4294967295.

**no-prepend**

Causes the device to stop prepending the selected ASN.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the local ASN.

## Examples

This example ensures that a device prepends the local ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100
```

This example stops the device from prepending the selected ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100 no-prepend
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor maxas-limit in

Causes the device to discard routes received in UPDATE messages if those routes exceed a maximum AS path length.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } maxas-limit in { num | disable }
no neighbor { ip-address | ipv6-address | peer-group-name } maxas-limit in
```

## Command Default

This command is disabled by default.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*num*

Maximum length of the AS path. Range is from 0 through 300. The default is 300.

**disable**

Prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead uses the default system value.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to remove this configuration.

## Examples

This example changes the length of the maximum allowed AS path length from the default.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 maxas-limit in 200
```



This example prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead use the default system value.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 maxas-limit in disable
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor maximum-prefix

Specifies the maximum number of IP network prefixes (routes) that can be learned from a specified neighbor or peer group.

## Syntax

**neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [ *threshold* ] [ **teardown** ]

**no neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [ *threshold* ] [ **teardown** ]

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*num*

Maximum number of IP prefixes that can be learned. Range is from 0 through 2147483647. Default is 0 (unlimited).

*threshold*

Specifies the percentage of the value specified by *num* that causes a syslog message to be generated. Range is from 1 through 100.

**teardown**

Tears down the neighbor session if the maximum number of IP prefixes is exceeded.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

The following example sets the maximum number of prefixes that will be accepted from the neighbor with the IP address 10.11.12.13 to 100000, and sets the threshold value to 80%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 maximum-prefix 100000 threshold 80
```

The following example, for VRF instance "red," sets the maximum number of prefixes that will be accepted from the neighbor with the IPv6 address 2001:2018:8192::125 to 100000, and sets the threshold value to 90%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 maximum-prefix 100000 threshold 90
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor next-hop-self

Causes the device to list itself as the next hop in updates that are sent to the specified neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } next-hop-self [ always ]  
no neighbor { ip-address | ipv6-address | peer-group-name } next-hop-self [ always ]
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

**always**

Enables this feature for route reflector (RR) routes.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to remove this configuration.

## Examples

This example causes all updates destined for the neighbor with the IP address 10.11.12.13 to advertise this device as the next hop.

```
device# configure terminal  
device(config)# router bgp  
device(config-bgp-router)# neighbor 10.11.12.13 next-hop-self
```

This example, for the VRF instance "red," causes all updates destined for the neighbor with the IPv6 address 2001:2018:8192::125 to advertise this device as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 next-hop-self
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor password

Specifies an MD5 password for securing sessions between the device and a neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } password string
no neighbor { ip-address | ipv6-address | peer-group-name } password
```

## Command Default

No password is set.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*string*

Password of up to 63 characters in length that can contain any alphanumeric character.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to remove this configuration.

## Examples

This example specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 password s0M3P@55W0Rd
```

This BGP4+ example, for VRF instance "red," specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 2001:2018:8192::125 password s0M3P@55W0Rd
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor peer-group

Configures a BGP neighbor to be a member of a peer group.

## Syntax

```
neighbor { ip-address | ipv6-address } peer-group string
no neighbor { ip-address | ipv6-address } peer-group string
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor.

**peer-group** *string*

Specifies the name of a BGP peer group. The name can be up to 63 characters in length and can be composed of any alphanumeric character.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to remove a neighbor from the peer group.

## Examples

This example assigns a specified neighbor to a peer group called "mypeergroup1".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 peer-group mypeergroup1
```

This BGP4+ example, for VRF instance "red," assigns a specified neighbor to a peer group called "mypeergroup1".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u)# neighbor 2001:2018:8192::125 peer-group mypeergroup1
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor prefix-list

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to IP address and mask length.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } prefix-list string { in | out }
```

```
no neighbor { ip-address | ipv6-address | peer-group-name } prefix-list string { in | out }
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*string*

Name of the prefix list. Range is from 1 through 63 ASCII characters.

**in**

Applies the filter in incoming routes.

**out**

Applies the filter in outgoing routes.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

This example applies the prefix list "myprefixlist" to incoming advertisements to neighbor 10.11.12.13 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 prefix-list myprefixlist in
```

This example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 2001:2018:8192::125 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

This example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 2001:2018:8192::125 for VRF instance "red,".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor remote-as

Specifies the autonomous system (AS) in which a remote neighbor resides.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } remote-as num
no neighbor { ip-address | ipv6-address | peer-group-name } remote-as
```

## Command Default

No AS is specified.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*num*

Remote AS number (ASN). Range is from 1 through 4294967295.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of this command to remove the neighbor from the AS.

## Examples

The following example specifies AS 100 for a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# neighbor 10.11.12.13 remote-as 100
```

The following BGP4+ example, for VRF instance "red," specifies AS 100 for a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 remote-as 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor remove-private-as

Configures a device to remove private autonomous system numbers (ASNs) from UPDATE messages that the device sends to a neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } remove-private-as
no neighbor { ip-address | ipv6-address | peer-group-name } remove-private-as
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor** *peer-group-name* command.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

The device will remove ASNs 64512 through 65535 (the well-known BGP4 private ASNs) from the AS-path attribute in UPDATE messages that the device sends to a neighbor.

## Examples

This example removes private ASNs globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remove-private-as
```

This example removes private ASNs for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 remove-private-as
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor route-map

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to a set of attributes defined in a route map.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } route-map { in string | out string }
no neighbor { ip-address | ipv6-address | peer-group-name } route-map { in string | out string }
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

**in**

Applies the filter on incoming routes.

*string*

Name of the route map. Range is from 1 through 63 ASCII characters.

**out**

Applies the filter on outgoing routes.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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



## Examples

The following example applies a route map named "myroutemap" to an outgoing route from 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 route-map out myroutemap
```

The following example applies a route map named "myroutemap" to an incoming route from 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 route-map in myroutemap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor route-reflector-client

Configures a neighbor to be a route-reflector client.

## Syntax

**neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

**no neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use this command on a host device to configure a neighbor to be a route-reflector client. Once configured, the host device from which the configuration is made acts as a route-reflector server.

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

## Examples

The following example configures a neighbor to be a route-reflector client.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 route-reflector-client
```

The following example configures a neighbor to be a route-reflector client for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 2001:2018:8192::125 route-reflector-client
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor send-community

Enables sending the community attribute in updates to the specified BGP neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } send-community [ both | extended | standard ]
no neighbor { ip-address | ipv6-address | peer-group-name } send-community [ both | extended | standard ]
```

## Command Default

The device does not send community attributes.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

**both**

Sends both standard and extended attributes.

**extended**

Sends extended attributes.

**standard**

Sends standard attributes.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

If the **send-community** attribute is enabled after a BGP session has been established, the neighbor session must be cleared for this change to take effect.

## Examples

The following example sends standard community attributes to a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 send-community standard
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sends extended community attributes to a neighbor for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 send-community extended
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor shutdown

Causes a device to shut down the session administratively with its BGP neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } shutdown [ generate-rib-out ]  
no neighbor { ip-address | ipv6-address | peer-group-name } shutdown [ generate-rib-out ]
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor** *peer-group-name* command.

**generate-rib-out**

When a peer is put into the shutdown state, Routing Information Base (RIB) outbound routes are not produced for that peer. Use this option to produce those routes.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

Shutting down a session lets you configure the neighbor and save the configuration without the need to establish a session with that neighbor.

## Examples

This example a device to shut down the session administratively with its neighbor.

```
device# configure terminal  
device(config)# router bgp  
device(config-bgp-router)# neighbor 10.11.12.13 shutdown
```

This example causes a device to shut down the session administratively with its neighbor and generate RIB outbound routes for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 shutdown generate-rib-out
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor soft-reconfiguration inbound

Stores all the route updates received from a BGP neighbor.

## Syntax

**neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

**no neighbor** { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor** *peer-group-name* command.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Soft reconfiguration stores all the route updates received from a neighbor. If you request a soft reset of inbound routes, the software compares the policies against the stored route updates, instead of requesting the neighbor's BGP4 or BGP4+ route table or resetting the session with the neighbor.

The **no** form of the command disables this feature.

## Examples

This example globally stores route updates from a BGP4 neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 soft-configuration inbound
```



This example stores route updates from a BGP4+ neighbor for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 soft-configuration inbound
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor static-network-edge

Overrides the default BGP4 behavior and advertises the network to a neighbor or peer group only when the corresponding route is installed as a forward route in the routing table.

## Syntax

```
neighbor { ip-address | peer-group-name } static-network-edge
no neighbor { ip-address | peer-group-name } static-network-edge
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

## Usage Guidelines

A BGP static network is always advertised to neighbors or a peer group, and if the corresponding route is not present in the routing table, BGP installs the null0 route. This command overrides the default behavior. This command is not supported for BGP4+.

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

## Examples

The following example globally overrides the default BGP4 behavior.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 static-network-edge
```

The following example overrides the default BGP4 behavior for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 10.11.12.13 static-network-edge
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor timers

Specifies how frequently a device sends KEEPALIVE messages to its BGP neighbors, as well as how long the device waits for KEEPALIVE or UPDATE messages before concluding that a neighbor is dead.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } timers keep-alive keepalive_interval hold-time holdtime_interval
no neighbor { ip-address | ipv6-address | peer-group-name } timers keep-alive keepalive_interval hold-time holdtime_interval
```

## Command Default

The keep-alive timer is 60 seconds. The hold timer is 180 seconds.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

**keep-alive** *keepalive\_interval*

Frequency (in seconds) with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

**hold-time** *holdtime\_interval*

Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

This example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

This example sets the keepalive timer to 120 seconds and the hold-timer to 360 seconds for VRF instance "red" .

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor unsuppress-map

Removes route suppression from BGP neighbor routes when those routes have been suppressed as a result of aggregation. All routes matching route-map rules are unsuppressed.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } unsuppress-map string
no neighbor { ip-address | ipv6-address | peer-group-name } unsuppress-map string
```

## Command Default

This feature is disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor.

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*string*

Name of the route map. Range is from 1 through 63 ASCII characters.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

The following BGP4 example removes route suppression for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 unsuppress-map myroutemap
```

The following BGP4+ example removes route suppression for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 unsuppress-map myroutemap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor update-source

Configures the BGP device to communicate with a neighbor through a specified interface.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } update-source { ip-address | ethernet slot / port | loopback num |
ve-interface vlan_id }
```

```
no neighbor { ip-address | ipv6-address | peer-group-name } update-source { ip-address | ethernet slot / port | loopback
num | ve-interface vlan_id }
```

## Command Default

Disabled.

## Parameters

*ip-address*

IPv4 address of the neighbor

*ipv6-address*

IPv6 address of the neighbor

*peer-group-name*

Peer group name configured by the **neighbor peer-group-name** command.

*ip-address*

IP address of the update source.

**ethernet**

Specifies an ethernet interface.

*slot*

Specifies a valid slot number.

*port*

Specifies a valid port number.

**loopback num**

Specifies a loopback interface.

**ve-interface vlan\_id**

Specifies a virtual Ethernet VLAN interface.

## Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode



## Usage Guidelines

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

## Examples

The following example configures the device to communicate with a neighbor through the specified IPv4 address and Ethernet interface 3/2.

```
device#configure terminal
device#(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 update-source ethernet 3/2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# neighbor weight

Specifies a weight that the device will add to routes that are received from the specified BGP neighbor.

## Syntax

```
neighbor { ip-address | ipv6-address | peer-group-name } weight num
no neighbor { ip-address | ipv6-address | peer-group-name } weight
```

## Command Default

The default for *num* is 0.

## Parameters

*ip-address*  
IPv4 address of the neighbor.

*ipv6-address*  
IPv6 address of the neighbor

*peer-group-name*  
Name of the peer group.

*num*  
Value from 1 through 65535.

## Modes

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

## Usage Guidelines

Use the **no** form of the command to restore the defaults.  
 BGP prefers larger weights over smaller weights.

## Examples

This example changes the weight from the default.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 weight 100
```

This example changes the weight from the default for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 weight 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# net

Configures an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process.

## Syntax

**net** *NSAP address*

**no net** *NSAP address*

## Command Default

900 seconds (15 minutes).

## Parameters

*NSAP address*

Specifies a Network Service Access Point (NSAP) address; composed of both an area ID and a system ID.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The *area-id* parameter specifies the area and has the format *xx* or *xx.xxxx*. For example, 49 and 49.2211 are valid area IDs.

The *system-id* parameter specifies the device's unique IS-IS router ID and has the format *xxxx.xxxx.xxxx*. You can specify any value for the system ID. A common practice is to use the base MAC address of the device as the system ID. The base MAC address is also the MAC address of port 1.

You must use the same system ID in all the NETs on the device.

The **no** form of the command removes the configured NET.

## Examples

The following example configures a NET that has the area ID 49.2211, the system ID 0000.00bb.cccc (the base MAC address), and the SEL value 00.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# net 49.2211.0000.00bb.cccc.00
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# network

Configures the device to advertise a BGP network.

## Syntax

**network** *network/mask* [ **backdoor** | **route-map** *map-name* | **weight** *num* ]

**no network** *network/mask* [ **backdoor** | **route-map** *map-name* | **weight** *num* ]

## Command Default

No network is advertised.

## Parameters

*network/mask*

Network and mask in CIDR notation.

**backdoor**

Changes administrative distance of the route to this network from the eBGP administrative distance (the default is 20) to the local BGP weight (the default is 200), tagging the route as a backdoor route.

**route-map** *map-name*

Specifies a route map with which to set or change BGP attributes for the network to be advertised. Range is from 1 through 63 ASCII characters.

**weight***num*

Specifies a weight to be added to routes to this network. Range is 0 through 65535. The default is 0.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

## Examples

This example imports the IP prefix 10.1.1.1/32 into the BGP4 database and specifies a route map called "myroutemap".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# network 10.1.1.1/32 route-map myroutemap
```

This example imports the IPv6 prefix 2001:db8::/32 into the BGP4+ database and sets a weight of 300.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# network 2001:db8::/32 weight 300
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# next-hop-enable-default

Configures the device to use the BGP default route as the next hop.

## Syntax

```
next-hop-enable-default
no next-hop-enable-default
```

## Command Default

This feature is disabled.

## Modes

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

## Usage Guidelines

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

## Examples

This BGP4 example configures the device to use the default route as the next hop for the default VRF.

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

This BGP4+ example configures the device to use the default route as the next hop for the default VRF.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# next-hop-mpls

Configures BGP shortcuts using next-hop MPLS to force BGP to use an MPLS tunnel as the preferred route to a destination network when an MPLS LSP tunnel is available.

## Syntax

```
next-hop-mpls [ compare-lsp-metric | follow-igp ]
```

```
no next-hop-mpls [ compare-lsp-metric | follow-igp ]
```

## Command Default

BGP uses the default BGP decision process and native IP forwarding to build BGP EMCP routes. Only IP routing tables are used to resolve routes for the routing table.

## Parameters

### compare-lsp-metric

Enables BGP to compare the configured LSP metrics as the IGP cost for the next hop.

### follow-igp

Ignores the MPLS metric cost in the BGP decision process and uses the IGP cost. BGP checks when an MPLS LSP is present, and totally ignores the LSP metric.

## Modes

BGP address-family IPv4 unicast configuration mode

## Usage Guidelines

When the **next-hop-mpls** command is enabled without either option, BGP sets the LSP metrics to one.

Enabling or disabling an option takes effect immediately. BGP automatically recalculates the existing BGP routes.

The **compare-lsp-metric** and **follow-igp** options are mutually exclusive.

When the **compare-lsp-metric** option is configured and you change the LSP metric, the routing table is updated.

Use the **no** form of the command to disable global next-hop MPLS.

When you use the **no** form of the command with the **compare-lsp-metric** or **follow-igp** option, all LSP metrics become equal cost. However, global next-hop MPLS remains enabled.

For the **follow-igp** option, consider the following:

- When you are running IGP throughout the network, and the IGP metric is trusted in the entire domain, you may want to rely on this IGP metric to make a best path and forwarding decision, regardless of whether the forwarding happens in native IP or MPLS encapsulation.
- The MPLS metric is manually configured in each LSP. There is no dynamic way to tie MPLS metric with an IGP metric. When using MPLS LSP as a BGP route outgoing interface, you loses the ability to tie the forwarding decision with a unified IGP metric.



- When combined with the BGP **install-igp-cost** command, you can change the route cost from BGP MED to IGP cost and is used when BGP routes are added to the RTM.
- When combined with a BGP outbound policy for route **set metric-type internal** command, you can set Layer-3 VPN and IP over MPLS routes using IGP metric to send out as the BGP MED value.

## Examples

The following example enables BGP shortcuts through next-hop MPLS and BGP to set the next hop IGP cost to one instead of the actual LSP metric.

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

The following example enables BGP shortcuts through next-hop MPLS and BGP to use the configured LSP metrics as the IGP cost for the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-mpls compare-lsp-metric
```

The following example enables BGP shortcuts through next-hop MPLS and BGP to ignore the LSP metrics and to use the IGP cost for the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-mpls follow-igp
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# next-hop-recursion

Enables BGP recursive next-hop lookups.

## Syntax

`next-hop-recursion`

`no next-hop-recursion`

## Command Default

This feature is disabled.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

## Usage Guidelines

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

If the BGP next hop is not the immediate next hop, a recursive route lookup in the IP routing information base (RIB) is needed. With recursion, a second routing lookup is required to resolve the exit path for destination traffic. Use this command to enable recursive next-hop lookups.

## Examples

This example enables recursive next-hop lookups for BGP4.

```
device# configure terminal
device(config)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-recursion
```

This example enables recursive next-hop lookups for BGP4+.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# node

Penalizes all links originating from the node IP address.

## Syntax

```
node { ip_addr }
no node { ip_addr }
```

## Command Default

The command is disabled, by default.

## Parameters

*ip\_addr*

All links that originate from the specified IP address are penalized.

## Modes

MPLS CSPF-group configuration mode.

## Usage Guidelines

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

## Examples

The example below configures a fate sharing group and specifies node 10.1.1.1 as the penalizing IP address.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-group computation-mode add-penalty
device(config-router-mpls-policy)# exit
device(config-router-mpls)# cspf-group group3
device(config-router-mpls-cspf-group-group3)# penalty 100
device(config-router-mpls-cspf-group-group3)# from 10.1.1.1
device(config-router-mpls-cspf-group-group3)# link 10.1.1.1 10.1.1.2
device(config-router-mpls-cspf-group-group3)# subnet 10.1.2.0/24
device(config-router-mpls-cspf-group-group3)# node 10.1.1.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# nonstop-routing (IS-IS)

Enables nonstop routing (NSR) for Intermediate System-to-Intermediate System (IS-IS).

## Syntax

**nonstop-routing**

**no nonstop-routing**

## Command Default

Enabled

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command disables nonstop routing.

## Examples

The following example enables NSR for IS-IS on a device.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# nonstop-routing
```

The following example disables NSR for IS-IS on a device.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no nonstop-routing
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# nonstop-routing (OSPF)

Enables nonstop routing (NSR) for OSPF.

## Syntax

**nonstop-routing**

**no nonstop-routing**

## Command Default

Enabled.

## Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

The **no** form of the command disables non-stop routing.

## Examples

The following example re-enables NSR on a device.

```
device# configuration terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# nonstop-routing
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# notification-timer

Sets the length of the EOL notification timer for LDP-IGP synchronization.

## Syntax

**notification-timer** *milliseconds*

**no notification-timer** *milliseconds*

## Command Default

The default value is 60000 milliseconds.

## Parameters

*milliseconds*

Specifies the length of the EOL notification timer in milliseconds. Enter an integer from 100 to 120000.

## Modes

MPLS LDP end-of-lib (eol) configuration mode

## Usage Guidelines

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

## Examples

The following example configures the EOL notification timer to 80000 milliseconds.

```
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# end-of-lib
device(config-mpls-ldp-eol)# notification-timer 80000

device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# eol
device(config-router-mpls-ldp-eol)# notification-timer 80000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# openflow default-behavior send-to-controller

Configures the OpenFlow default behavior to send to controller.

## Syntax

```
openflow default-behavior send-to-controller
```

```
{no} openflow default-behavior send-to-controller
```

## Modes

Global configuration mode

## Usage Guidelines

The switch uses default behavior command for packets, which don't match any OpenFlow flows.

## Examples

To configure OpenFlow default behavior globally, enter the following command.

```
device(config)# openflow default-behavior send-to-controller
```

To disable the command, enter the following command.

```
device(config)# no openflow default-behavior send-to-controller
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# openflow enable

Enables the OpenFlow mode globally or on an interface. Configures OpenFlow hybrid mode on an interface.

## Syntax

```
openflow enable ofv13
```

```
openflow enable [ layer2 ][ layer3 ][ layer23 ][ hybrid-mode ]
```

```
{no} openflow enable
```

## Command Default

OpenFlow is disabled on the device.

## Parameters

**ofv13**

Specifies OpenFlow protocol 1.3.0.

**layer2**

Matches only on Layer 2 packet headers.

**layer3**

Matches only on Layer 3 packet headers.

**layer23**

Matches only on Layer 23 packet headers.

**hybrid-mode**

Specifies the OpenFlow hybrid mode.

## Modes

Global configuration mode

Interface configuration mode

## Usage Guidelines

When the switch connects to the controller the switch advertises the configured OpenFlow version to the controller.

An OpenFlow must be configured globally, before you configure on an interface.

To change from one mode to another, you disable the working mode and then configure the new mode.

Prerequisites to configure OpenFlow hybrid mode on an interface:

- Openflow must be enabled globally.
- Switchport must be configured on the interface.
- Switchport mode trunk must be configured on the interface.



## Examples

To enable OpenFlow globally, enter the following command.

```
device(config)# openflow enable ofv13
```

To enable OpenFlow on an interface and match on Layer 2 packet headers, enter the following command.

```
device(config)# Ethernet 3/1
device(conf-if-eth-3/1)# openflow enable layer2
```

To disable on Layer 2 packet headers, enter the following command.

```
device(conf-if-eth-3/1)# no openflow enable
```

To match on Layer 3 packet headers, enter the following command.

```
device(config)# Ethernet 3/2
device(conf-if-eth-3/2)# openflow enable layer3
```

To match on Layer 23 packet headers, enter the following command.

```
device(config)# Ethernet 3/3
device(conf-if-eth-3/3)# openflow enable layer23
```

To configure OpenFlow hybrid mode on an interface, enter the following command.

```
device(config)# interface Ethernet 3/1
device(conf-if-eth-3/1)# switchport
device(conf-if-eth-3/1)# switchport mode trunk
device(conf-if-eth-3/1)# openflow enable layer23 hybrid-mode
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# openflow-controller

Configures an OpenFlow controller in active connection mode.

## Syntax

**openflow-controller** *controller-name*

**openflow-controller** *ip-address* [ **no-ssl** | **ssl** ] [ **port** *port-number* ] [ **use-vrf** *vrf name* ]

**no openflow-controller** *controller-name*

## Command Default

See the Usage Guidelines.

## Parameters

*controller-name*

Specifies the user-given name for the controller.

**ip-address**

Specifies the IPv4 address of the controller.

**use-vrf**

Specifies the VRF name to connect to the OpenFlow controller.

**ssl**

Specifies an SSL connection.

**no-ssl**

Specifies a TCP connection.

**port** *port-number*

Specifies the OpenFlow controller TCP port number. Range is from 1 through 65535.

## Modes

Global configuration mode

## Usage Guidelines

SSL is default for the connection method. *no-ssl* option indicates to use TCP instead of SSL. The default port is 6633.

If no VRF name is specified, *mgmt-vrf* is the default VRF.

Use the **no** form of the command to remove the specified OpenFlow controller. You cannot remove an active controller.

## Examples

This example creates an OpenFlow controller and assigns an IPv4 address and port.

```
device(config)# openflow controller A1 ip-address 10.25.128.185 no-ssl port 9000
device(config)# openflow controller A2 ip-address 10.25.128.185 no-ssl
device(config)# no openflow controller A2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# openflow protected-vlans

Configures an OpenFlow protected VLAN.

## Syntax

```
openflow protected-vlans add[vlan id | vlan range]
```

```
openflow protected-vlans remove [vlan id | vlan range]
```

## Command Default

See the Usage Guidelines.

## Parameters

**vlan id**

Specifies the VLAN ID of the interface.

**vlan range**

Specifies the range of VLAN IDs of the interface.

## Modes

Global configuration mode

## Usage Guidelines

OpenFlow protected VLANs can be preconfigured even when OpenFlow is not enabled on the interface.

If protected VLAN is configured on the interface, only OpenFlow hybrid mode can be configured on that interface.

## Examples

This example adds the VLANs on the interface.

```
device(config)# interface Ethernet 3/1
device(conf-if-eth-3/1)# openflow protected-vlans add 201, 204, 206
```

This example adds the VLAN range on the interface.

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# openflow protected-vlans add 10-20
```

To remove protected VLANs from the interface, use this command.

```
device(conf-if-eth-3/2)# openflow protected-vlans remove 10-20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# oscmd

Runs commands or user-defined scripts supported by the Linux OS directly from the CLI.

## Syntax

```
oscmd { Linux-command | script-name }
```

## Parameters

*Linux-command*

Specifies the Linux command that you want to run.

*script-name*

Specifies the user-defined script that you want to run.

## Modes

Privileged EXEC

## Usage Guidelines

This command is only visible in the CLI when you are configured as a user with the admin role.

All scripts run under **oscmd** must have execute permission.

After writing and testing a user-defined script file, you can copy it to the Extreme device. Imported scripts are stored in the `/var/config/vcs/scripts` directory.

You can also create scripts from the Linux shell using the "vi" editor. The newly-created scripts must exist in the `/fabos/users/admin` directory.

When you use the **oscmd** command, the execution of the following Linux commands are not supported:

- **bash**
- **chgrp**
- **chmod**
- **chown**
- **cp**
- **kill**
- **killall**
- **mv**
- **rm**
- **rmdir**
- **sh**
- **script**
- **vi**
- **vim**

## Examples

In the following example, the Linux **ps -ef** command lists the process status from the CLI.

```
device# oscmd ps -ef
UID      PID  PPID  C  STIME TTY          TIME CMD
root      1    0    0  Jul24 ?           00:00:04 /sbin/init
root      2    0    0  Jul24 ?           00:00:00 [kthreadd]
root      3    2    0  Jul24 ?           00:00:00 [migration/0]
root      4    2    0  Jul24 ?           00:00:03 [ksoftirqd/0]
root      5    2    0  Jul24 ?           00:00:00 [migration/1]
root      6    2    0  Jul24 ?           00:00:03 [ksoftirqd/1]
root      7    2    0  Jul24 ?           00:00:00 [migration/2]
root      8    2    0  Jul24 ?           00:00:02 [ksoftirqd/2]
root      9    2    0  Jul24 ?           00:00:00 [migration/3]
root     10    2    0  Jul24 ?           00:00:02 [ksoftirqd/3]
root     11    2    0  Jul24 ?           00:00:00 [migration/4]
root     12    2    0  Jul24 ?           00:00:02 [ksoftirqd/4]
root     13    2    0  Jul24 ?           00:00:00 [migration/5]
root     14    2    0  Jul24 ?           00:00:03 [ksoftirqd/5]
root     27    2    0  Jul24 ?           00:00:00 [cpuset]
root     28    2    0  Jul24 ?           00:00:01 [khelper]
root     31    2    0  Jul24 ?           00:00:00 [netns]
root     34    2    0  Jul24 ?           00:00:00 [async/mgr]
root    270    2    0  Jul24 ?           00:00:00 [sync_supers]
root    272    2    0  Jul24 ?           00:00:00 [bdi-default]

...

root      8kblockd/6]182      1  0  Jul24 ?           00:00:00 /usr/sbin/inetd
root      8237      1  0  Jul24 ?           00:00:00 /usr/sbin/sshd
admin    27536 27535  0  04:19 pts/4           00:00:00 ps -ef
```

In the following example, `<my_script>` is the name of a user-defined script that exists in the `/fabos/users/admin` directory and is executable under the Linux OS or downloaded by using the `copy` command.

```
device# oscmd <my_script>
```

## History

Release version	Command history
16r.1.00	This command was introduced.
16r.1.01	This command was modified to add user-defined script information and a list of unsupported Linux commands.
16r.1.01a	This topic was modified to add <b>cp</b> and <b>mv</b> to the list of unsupported Linux commands.

# overlay access-group

Configures an overlay access-list under overlay-transit.

## Syntax

```
overlay access-group overlay-vxlan-acl-name in
no overlay access-group
```

## Parameters

*overlay-vxlan-acl-name*

The overlay access-list name.

in

Applies overlay access-list to ingress traffic.

## Modes

Overlay-transit mode.

## Usage Guidelines

You must create an overlay access-list before to apply under overlay-transit.

Use the **no** form of this command to delete the overlay access list.

## Examples

This example creates an overlay access list.

```
device # configure terminal
device(config)# overlay-transit tr_name
device(config-overlay-transit-tr_name)# overlay access-group abc_ext in
```

This example deletes an overlay access list.

```
device(config-overlay-transit-vxlan1)# no overlay access-group abc_ext
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# overlay access-list type vxlan extended

Creates an access-list with extended headers for deep inspection. Extended access-list allows to configure VXLAN tunnel endpoints (VTEP source and destination IP), VNI and VNI IP range, inner source and destination IP and networks and inner source and destination ports.

## Syntax

```
overlay access-list type vxlan extended user-acl-name
no overlay access-list type vxlan extended user-acl-name
```

## Parameters

*user-acl-name*  
Specifies the user ACL name.

## Modes

Global configuration mode.

## Usage Guidelines

Use the **no** form of this command to delete an extended access-list.

## Examples

This example creates an extended access-list.

```
device# configure terminal
device(config)# overlay access-list type vxlan extended abc_ext
2016/08/15-23:29:09, [SSMD-1400], 4282, M1 | Active | DCE, INFO, SLX, Overlay access list abc_ext is
created.
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# overlay access-list type vxlan standard

Enables configuring only the VXLAN tunnel endpoint (VTEP) IP address and VXLAN Network Identifier (VNI) to match.

## Syntax

```
overlay access-list type vxlan standard user-acl-name
```

```
no overlay access-list type vxlan standard user-acl-name
```

## Parameters

*user-acl-name*

The user ACL name.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no** form of this command to delete a standard access-list.

## Examples

This example creates a standard access-list.

```
device# configure terminal
device(config)# overlay access-list type vxlan standard overlay_vxlan_std
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# overlay-transit

Configures an overlay transit.

## Syntax

```
overlay-transit overlay-transit-name
```

```
no overlay-transit overlay-transit-name
```

## Parameters

*overlay-transit-name*

The overlay transit name.

## Modes

Global configuration mode.

## Usage Guidelines

Use the **no** form of this command to delete the overlay transit configuration.

## Examples

This example configures an overlay transit.

```
device# configure terminal
device(config)# overlay-transit vlx_transit
```

This example deletes an overlay transit configuration.

```
device(config)# no overlay-transit vlx_transit
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# partial-spf-interval

Changes the partial shortest path first (PSPF) interval.

## Syntax

```
partial-spf-interval max-wait initial-wait second-wait  
no partial-spf-interval
```

## Parameters

*max-wait*

Specifies the maximum interval in seconds between SPF recalculations. The range is from 0 through 120 seconds. The default is 5 seconds.

*initial-wait*

Specifies the initial SPF calculation delay in milliseconds after an LSP change. The range is from 0 through 120000 milliseconds. The default for this variable is value of the *max-wait* time.

*second-wait*

Indicates the hold time between the first and second SPF calculation in milliseconds. The range is from 1 through 120000 milliseconds. The default is 5000 milliseconds (5 seconds). The default for this variable is value of the *max-wait* time.

## Modes

IS-IS router configuration mode

## Usage Guidelines

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

## Examples

The following example specifies that the maximum interval between SPF recalculations is 15 seconds, the initial SPF calculation delay is 10000 milliseconds, and the hold time between the first and second SPF calculation is 15000 milliseconds.

```
device# configure terminal  
device(config)# router isis  
device(config-isis-router)# partial-spf-interval 15 10000 15000
```

The following example restores the default values.

```
device# configure terminal  
device(config)# router isis  
device(config-isis-router)# no partial-spf-interval
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# password-attributes

Configures global password attributes.

## Syntax

```
password-attributes { [ max-retry maxretry ] [ min-length minlen ] [ max-lockout-duration duration ] [ admin-lockout |
character-restriction { [ lower numlower ] [ numeric numdigits ] [ special-char numsplchars ] [ upper numupper ] } } }
no password-attributes { [ max-retry maxretry ] [ min-length minlen ] [ max-lockout-duration duration ] [ admin-lockout |
character-restriction { [ lower numlower ] [ numeric numdigits ] [ special-char numsplchars ] [ upper numupper ] } } }
```

## Command Default

The default for *min-length* is 8. All other defaults are 0.

## Parameters

### admin-lockout

Enables lockout for admin role accounts.

### character-restriction

Configures the restriction on various types of characters.

#### lower *numlower*

Specifies the minimum number of lowercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

#### numeric *numdigits*

Specifies the minimum number of numeric characters that must occur in the password. Values range from 0 through 32 characters. The default is 0.

#### special-char *numsplchars*

Specifies the number of punctuation characters that must occur in the password. All printable, nonalphanumeric punctuation characters, except colon (:) are allowed. Values range from 0 through 32 characters. The default value is 0.

#### upper *numupper*

Specifies the minimum number of uppercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

### max-retry *maxretry*

Specifies the number of failed password logins permitted before a user is locked out. Values range from 0 through 16 attempted logins. The default value is 0.

### min-length *minlen*

Specifies the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

### max-lockout-duration *duration*

Specifies the maximum number of minutes after which the user account is unlocked. Range is from 0 through 99999. The default is 0, representing an infinite duration.

## Modes

Global configuration mode

## Usage Guidelines

To reset password attributes to their default values, enter the **no** form of this command.

## Examples

The following example configures global password attributes and verifies the configuration.

```
device#configure terminal
device(config)# password-attributes max-retry 4
device(config)# password-attributes character-restriction lower 2
device(config)# password-attributes character-restriction upper 1 numeric 1 special-char 1
device(config)# exit
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

The following example resets the character restriction attributes and verifies the configuration.

```
device#configure terminal
device(config)# no password-attributes character-restriction lower
device(config)# no password-attributes character-restriction upper
device(config)# exit
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

The following example clears all global password attributes.

```
device#configure terminal
device(config)# no password-attributes
device(config)# exit
device# show running-config password-attributes

% No entries found.
```

The following example sets the maximum number of retries to 3 and enables lockout policy for admin role accounts.

```
device#configure terminal
device(config)# password-attributes max-retry 3 admin-lockout
```

The following example specifies that the user account be unlocked after 5 minutes and enables lockout policy for admin role accounts.

```
device#configure terminal
device(config)# password-attributes max-lockout-duration 5 admin-lockout
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# path

A path is a list of router hops that specifies a route across an MPLS domain. Once the user creates a path, the user can create signaled LSPs that see the path.

## Syntax

```
path { path_name } [ hop ip_addr ] | [ [ insert ip_addr ] [ [ loose | strict ] ip_addr ] ]
no path { path_name } [ hop ip_addr ] | [ [ insert ip_addr ] [ [ loose | strict ] ip_addr ] ]
```

## Command Default

No paths are modified by default.

## Parameters

*path\_name*

Specifies the selected path name.

hop *ip\_addr*

Configures the specified the strict or loose hop.

insert *ip\_addr*

Specifies the inserted path strict or loose hop.

loose *ip\_addr*

There can be other routers in between.

strict *ip\_addr*

The router must be directly connected to the preceding node.

## Modes

MPLS path mode (config-router-mpls-path-name).

## Usage Guidelines

The no form of the command removes the specified path.

A path is always configured at the ingress LER and assumes that the ingress LER is the beginning of the path. A path can contain any number of nodes, which correspond to MPLS-enabled routers in the network.

## Examples

The following example configures a path called sf\_to\_sj that has four nodes.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# path sf_to_sj
device(config-router-mpls-path-sf_to_sj)# hop 2.3.4.5 strict
device(config-router-mpls-path-sf_to_sj)# hop 1.2.3.4 strict
device(config-router-mpls-path-sf_to_sj)# exit
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## peer

Configures a peer IP address in a bridge domain. A corresponding pseudowire (PW) interface is created when the peer IP address is configured.

## Syntax

```
peer ip-address [ cos num ] [ load-balance ] [ lsplsp-name1, lsp-name2,...lsp-name32 ]
```

```
no peer [ ip-address ]
```

## Command Default

No PW interfaces are configured.

## Parameters

*ip-address*

Specifies a PW IP address for a remote peer.

**cos** *num*

Specifies a Class of Service (CoS) value for selecting a label-switched path to reach the peer. The range is from 0 through 7.

**load-balance**

Specifies load balancing. Up to 16 alternate paths are used for load balancing.

**lsp** *lsp-name1, lsp-name2,...lsp-name32*

Specifies the name of a label-switched path. Up to 32 label-switched path names can be configured.

## Modes

Bridge-domain configuration mode.

## Usage Guidelines

The virtual connection identifier (VC ID) must be configured by using the **vc-id** command prior to configuring the peer IP address to create a PW interface.

The **no** form of the command deletes the peer IP address configuration and the PW interface that corresponds with the specified peer IP address.

The following configuration combinations are allowed:

- **peer** *ip-address* **cos**
- **peer** *ip-address* **cos** **load-balance**
- **peer** *ip-address* **load-balance**
- **peer** *ip-address* **load-balance** **cos**
- **peer** *ip-address* **load-balance** **lsp** *lsp-name1, lsp-name2,...lsp-name32*
- **no peer** *ip-address*

- **no peer ip-address lsp** *lsp-name1, lsp-name2,...lsp-name32*

#### NOTE

When a peer is already configured, you cannot add a CoS or load balance configuration. To configure a CoS value or load balancing, the peer must be removed by using the **no peer** command and re-configured specifying the required **cos** or **load-balance** options.

To remove the CoS or load-balance configuration, the peer configuration must be removed by using the **no peer** command.

## Examples

The following example shows how to configure a peer IP address (10.12.12.12) for bridge domain 1 with the **load-balance** option.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.12.12.12 load-balance
```

The following example shows how to configure a peer IP address (10.12.12.12) for bridge domain 1 specifying two label-switched paths (lsp1 and lsp2).

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.12.12.12 lsp lsp1 lsp2
```

The following example shows how to configure a peer IP address (10.1.1.1) for bridge domain 1 specifying load balancing and four label-switched paths (lsp1, lsp2, lsp3 and lsp4).

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.1.1.1 load-balance lsp lsp1 lsp2 lsp3 lsp4
```

The following example shows the error message that displays when you try to configure the **load-balance** option for an existing peer. The peer configuration must be removed and reconfigured to specify the **load-balance** option as shown in the example.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 15.15.15.15
device(config-bridge-domain-1)# peer 15.15.15.15 load-balance
Error: can not configure load-balance on existing peer.
device(config-bridge-domain-1)#no peer 15.15.15.15
device(config-bridge-domain-1)# peer 15.15.15.15 load-balance
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# peer (MCT)

Configures the IP address for the MCT cluster peer.

## Syntax

```
peer ip-address
no peer [ ip-address ]
```

## Parameters

*ip-address*

Specifies the IP address for the cluster peer. The address is either the peer loopback address or nexthop IP address.

## Modes

Cluster configuration mode.

## Usage Guidelines

Configure a corresponding neighbor in BGP EVPN address family for the peer. If the peer is already configured as a neighbor, when you deploy and undeploy the cluster, the BGP neighbor resets to renegotiate its capability.

If the peer already exists for other address family, clear the IP BGP peer session.

The **no** form of the command deletes the peer IP address configuration.

## Examples

The following example shows the configuring of the cluster peer IP address.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# peer 10.10.10.12
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# peer-interface

Configures the Ethernet or VE interface to reach the MCT cluster peer.

## Syntax

```
peer-interface Ethernet slot/port | Ve number
no peer-interface
```

## Parameters

**Ethernet** *slot/port*  
Specifies the Ethernet interface for the cluster peer.

**Ve** *number*  
Specifies the VE interface for the cluster peer.

## Modes

Cluster configuration mode.

## Usage Guidelines

The **no** form of the command deletes the peer interface configuration.

You must configure the peer interface before deploying the cluster configuration.

You cannot change the peer interface when the cluster is deployed.

## Examples

The following example shows the configuring of the cluster peer interface.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# peer-interface Ve 20
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# penalty

Sets the penalty value for a CSPF fate-sharing group.

## Syntax

```
penalty { penalty_value }
no penalty
```

## Command Default

The command is disabled by default.

## Parameters

*penalty\_value*

Specifies the penalty value that is assigned to objects of the same fate-sharing group. The range is from 1 through 65535. The default value is one (1). Objects of the same fate-sharing group share the same penalty value. For example, all objects in group 3 share the same penalty value of 100.

## Modes

MPLS CSPF group mode.

## Usage Guidelines

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

## Examples

The following example configures the penalty value to 100.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# cspf-group group3
device(config-router-mpls-cspf-group-group3)# penalty 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## police cir

Configures the committed information rate, committed burst size, exceeded information rate, and the exceeded burst size for the class map.

### Syntax

```
police cir cir-bps [ cbs bytes ] [ eir bps [ ebs bytes ] ]
no police { cir [ cbs ] [ eir [ ebs ] ] }
```

### Parameters

*cir-bps*

Specifies the committed information rate in bits per second. Enter an integer from 18000 to 300000000000.

*cbs bytes*

Specifies the committed burst size in bytes. Enter an integer from 1250 to 37500000000.

*eir bps*

Specifies the exceeded information rate in bits per second. Enter an integer from 0 to 300000000000.

*ebs bytes*

Specifies the exceeded burst size in bytes. Enter an integer from 1250 to 37500000000.

### Modes

Policy-map class configuration mode

### Usage Guidelines

Use the **no** version of this command to remove the parameter from the class map.

Only the **police cir** command is mandatory for configuring a class map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

### Examples

The following example sets the committed information rate (cir), committed burst size (cbs), exceeded information rate (eir), and the exceeded burst size (ebs).

```
device# configure terminal
device(config)# policy-map policy_2
device(config-policymap)# class default
device(config-policymap-class)# police cir 3000000 cbs 375000000 eir 300000000 ebs 37500000
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# policy-map

Configures a policy map containing a class map so that you can apply policer and QoS attributes to a particular interface.

## Syntax

```
policy-map policy-mapname
```

```
no policy-map policy-mapname
```

## Command Default

No policy map is created.

## Parameters

*policy-mapname*

Name of police policy map

## Modes

Global configuration mode

## Usage Guidelines

When you launch the **policy-map** command, the system is placed in `config-policymap mode` for the configured map. At this point, you can add a class map containing policing parameters to the policy map. (Refer to the description of the **class** command.)

This command creates a policer policy map to apply policer and QoS attributes to a particular interface. Each policy map can contain up to 32 class maps. The class map can be associated with specific policing and QoS parameters.

Maximum number of policy map creations are 128

Associate the policy map to the interface for inbound or outbound direction with the **service-policy** command.

Enter **no policy-map** *policy-mapname* while in global configuration mode to remove the policy map.

## Examples

Create a policy map and place system into config-policymap mode so that you can add a class map.

```
device# configure terminal
device(config)# policy-map policymap1
device(config-policymap)#
```

Remove the policy map while in global configuration mode.

```
device# configure terminal
device(config)# no policy-map policymap1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# port-channel path-cost

Sets the port channel path cost behavior.

## Syntax

```
port-channel path-cost [ custom | standard ]
```

## Command Default

Path cost is standard.

## Parameters

### custom

Specifies to use the custom behavior, which sets the path cost changes according to the port-channel's bandwidth.

### standard

Specifies to use the standard behavior, which sets that the path cost does not change according to port-channel's bandwidth.

## Modes

Spanning tree configuration mode

## Examples

To set the behavior for the path cost to custom:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# port-channel path-cost custom
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# port-channel path-cost custom
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# port-channel path-cost custom
```

```
device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# port-channel path-cost custom
```

```
device# configure terminal
device(config)# protocol spanning-tree rpvt
device(conf-rpvst)# port-channel path-cost custom
```

To set the behavior for the path cost to standard:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# port-channel path-cost standard
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# port-channel path-cost standard
```

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# port-channel path-cost standard
```

```
device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# port-channel path-cost standard
```

```
device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# port-channel path-cost standard
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# port-group

Accesses the port group mode for the port group of an SLX 9850 36x100G line card that you want to configure.

## Syntax

```
port-group slot/port-group
```

## Parameters

*slot/port-group*

Specified the slot and port group that you want to configure. To display the port groups, use the **show hardware port-group** command.

## Modes

Hardware configuration mode

## Usage Guidelines

Before changing the configuration of a port group, you must power off the line card.

## Examples

The following example accesses a port group.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# port-group 3/1
device(config-port-group-3/1)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# power-off

Powers off a line card or switch fabric module (SFM).

## Syntax

```
power-off { linecard slot_number } | { sfm slot_number }
```

## Parameters

**line card** *slot\_number*

Powers off the specified line card. For the SLX 9850-4 line-card slot number, enter an integer from 1 to 4. For the SLX 9850-8 line-card slot, enter an integer from 1 to 8.

**sfm** *slot\_number*

Powers off the specified SFM. For the SFM slot number, enter an integer from 1 to 6.

## Modes

Privileged EXEC mode

## Usage Guidelines

A line card must be powered off before you can change the slot configuration.

## Examples

The following example powers off the line card in slot 3.

```
device# power-off linecard 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## power-on

Powers on a line card or switch fabric module (SFM).

### Syntax

```
power-on { linecard slot_number } | { sfm slot_number }
```

### Parameters

**line card slot\_number**

Powers on the specified line card. For the SLX 9850-4 line-card slot number, enter an integer from 1 to 4. For the SLX 9850-8 line-card slot, enter an integer from 1 to 8.

**sfm slot\_number**

Powers on the specified SFM. For the SFM slot number, enter an integer from 1 to 6.

### Modes

Privileged EXEC mode

### Examples

The following example powers on the line card in slot 3.

```
device# power-on linecard 3
```

### History

Release version	Command history
16r.1.00	This command was introduced.



# preempt-mode

Enables or disables preempt mode for a VRRP or VRRP Extended (VRRP-E) router session.

## Syntax

**preempt-mode**

**no preempt-mode**

## Command Default

Enabled for VRRP; Disabled for VRRP-E.

## Modes

Virtual-router-group configuration mode

Virtual-router-extended-group configuration mode

## Usage Guidelines

This command is for VRRP and VRRP-E.

For VRRP-E, the interface must be a virtual interface (Ve).

When set, the highest-priority backup router will always be the master if the owner is not available. If not set, a higher priority backup will not preempt a lower-priority master.

Enter **no preempt-mode** to turn off preempt mode.

## Examples

To turn on preempt mode for a virtual-router-group 1 session:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 10
device(config-if-Ve-10)# ipv6 vrrp-extended-group 1
device(config-vrrp-extended-group-1)# preempt-mode
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# priority

Sets the priority of a physical router in a VRRP router group.

## Syntax

**priority** *range*

## Command Default

The default priority is 100.

## Parameters

*range*

The priority of a physical router in a virtual router group. Higher numbers have priority over lower numbers. Valid values range from 1 to 254.

## Modes

Virtual-router-group configuration mode

Virtual-router-extended-group configuration mode

## Usage Guidelines

You can perform this command for VRRP or VRRP-E.

When set, the highest priority backup router will always be the master. (For VRRP, however, the owner is always the master if it is available.) If not set, a higher priority backup will not preempt a lower priority backup that is acting as master.

For an owner router in VRRP, the priority automatically becomes 255 if the virtual IP address of the virtual router and the real IP address of the owner are the same.

## Examples

To set the priority to 110 for the VRRP virtual group 1:

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ve 10
device(config-if-Ve-10)# vrrp-group 1
device(config-vrrp-group-1)# priority 110
```

To set the priority to 110 for the VRRP-E virtual group 1:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 10
device(config-if-Ve-10)# ipv6 vrrp-extended-group 1
device(config-vrrp-extended-group-1)# priority 110
```

# History

Release version	Command history
16r.1.00	This command was introduced.

# process-restart

The MPLS process restart capability is a fault containment mechanism which ensures that process-level failures do not cause system-level failures.

## Syntax

`process-restart`

## Command Default

The command is disabled, by default.

## Modes

HA configuration mode (config-ha).

## Usage Guidelines

MPLS is a COLD restartable process, meaning when there is a fault inside the MPLS process, and it crashes, the system does not undergo a failover; instead, the MPLS process is restarted on the same ACTIVE MM. All the other modules and processes that interact with MPLS are made aware of the MPLS restart, and they adjust accordingly. All the MPLS-based services, such as IPoMPLS, VLL, VPLS are disrupted for the duration of MPLS process restart. Once MPLS process is restarted, the control protocols (LDP and RSVP) re-signal the tunnels and cross-connects and subsequently all the dependent MPLS applications to resume service.

## Examples

The following example disables the process-restart command.

```
device# configure
device(config)# ha
device(config-ha)# process-restart disable mpls
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# profile

Creates an LLDP profile.

## Syntax

**profile** *name*

**no profile** *name*

## Parameters

*name*

Assigns a name to the profile. The name must be between 1 and 63 ASCII characters in length.

*name*

Assigns a name to the profile. The name must be between 1 and 32 ASCII characters in length.

## Modes

Protocol LLDP configuration mode

## Usage Guidelines

When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile. Up to 64 profiles can be created.

Enter **no profile** *name* to remove the named profile.

## Examples

The following example creates a profile named test.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# profile test
```

The following example creates a profile named test1.

```
device(config)# protocol lldp
device(conf-lldp)# profile ?
Possible completions:
<Profile Name (Max Size - 32)>
device(conf-lldp)# profile test1
device(config-profile-test1)#
```

The following example deletes a profile named test:

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# no profile test
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# protocol

Configures the authentication protocol to use for communication with the Remote Authentication Dial-In User Service (RADIUS) server.

## Syntax

```
protocol { chap | pap | peap }
no protocol
```

## Command Default

The default protocol is Challenge Handshake Authentication Protocol (CHAP).

## Parameters

- chap**  
Specifies using CHAP for communication with the RADIUS server.
- pap**  
Specifies using Password Authentication Protocol (PAP) for communication with the RADIUS server.
- peap**  
Specifies using Protected Extensible Authentication Protocol (PEAP) for communication with the RADIUS server.

## Modes

RADIUS server host VRF configuration mode

## Usage Guidelines

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

## Examples

The following example shows how to configure PAP as the authentication protocol for communication with the RADIUS server.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# protocol pap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# protocol lldp

Enters the Link Layer Discovery Protocol (LLDP) configuration mode.

## Syntax

```
protocol lldp
```

```
no protocol lldp
```

## Command Default

LLDP protocols are enabled.

## Modes

Global configuration mode

## Usage Guidelines

Enter **no protocol lldp** to restore the default settings.

## Examples

To enter LLDP mode:

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

To reset all LLDP configurations:

```
device# configure terminal
device(config)# no protocol lldp
device(conf-lldp)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# protocol spanning-tree

Designates the context for spanning tree.

## Syntax

```
protocol spanning-tree { mstp | rstp | stp | pvst | rpvst }  
no protocol spanning-tree
```

## Command Default

STP is not enabled. STP is not required in a loop-free topology.

## Parameters

<b>mstp</b>	Specifies the Multiple Spanning Tree Protocol (MSTP).
<b>rstp</b>	Specifies the Rapid Spanning Tree (RSTP).
<b>stp</b>	Specifies the Spanning Tree Protocol (STP).
<b>pvst</b>	Specifies Per-VLAN Spanning Tree Protocol Plus (PVST+).
<b>rpvst</b>	Specifies Rapid Per-VLAN Spanning Tree Protocol Plus (R-PVST+).

## Modes

Global configuration mode

## Usage Guidelines

Consider enabling STP to detect or avoid loops. You must turn off one form of STP before turning on another form.

Packet drops or packet flooding may occur if you do not enable xSTP on all devices connected on both sides of parallel links.

Enter **no protocol spanning-tree** to delete the context and all the configurations defined within the context or protocol for the interface.

## Examples

To enable the Spanning Tree Protocol:

```
device# configure terminal  
device(config)# protocol spanning-tree stp
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# protocol uddl

Enables and/or enters unidirectional link detection (UDLD) protocol configuration mode.

## Syntax

```
protocol uddl
```

```
no protocol uddl
```

## Command Default

This protocol is disabled by default.

## Modes

Global configuration mode

## Usage Guidelines

UDLD detects and blocks a physical link that becomes unidirectional. A unidirectional link can cause traffic in a network to loop endlessly. When the link becomes bidirectional again, UDLD unblocks the link.

This protocol applies only to physical ports. In addition to running this command, you must also enable each desired port for UDLD in interface subconfiguration mode.

Use the **no protocol uddl** command to disable the UDLD protocol and revert all UDLD configuration to defaults.

## Examples

To enable the unidirectional link detection (UDLD) protocol:

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

# protocol vrrp

Globally enables Virtual Router Redundancy Protocol (VRRP).

## Syntax

```
protocol vrrp
```

```
no protocol vrrp
```

## Command Default

VRRP is not enabled.

## Modes

Global configuration mode

## Usage Guidelines

The **no** form of this command globally disables VRRP.

## Examples

To enable VRRP:

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# protocol vrrp-extended

Globally enables VRRP-Extended.

## Syntax

```
protocol vrrp-extended
no protocol vrrp-extended
```

## Command Default

Disabled

## Modes

Global configuration mode

## Usage Guidelines

The **no protocol vrrp-extended** command globally disables VRRP-E.

## Examples

To enable VRRP-Extended:

```
device# configure terminal
device (config)# protocol vrrp-extended
```

# prune-wait

Configures the time a PIM device waits before stopping traffic to neighbor devices that do not want the traffic.

## Syntax

**prune-wait** *seconds*

**no prune-wait**

## Command Default

The prune wait time is 3 seconds.

## Parameters

*seconds*

Specifies the wait time in seconds. The range is 0 through 30 seconds. The default is 3 seconds.

## Modes

PIM router configuration mode

## Usage Guidelines

A smaller prune wait value reduces flooding of unwanted traffic. A prune wait value of 0 causes the PIM device to stop traffic immediately upon receiving a prune message.

If there are two or more neighbors on the physical port, you should not configure the **prune-wait** command because one neighbor may send a prune message while the other sends a join message at the same time, or within less than 3 seconds.

The **no** form of this command restores the default prune wait time of 3 seconds.

## Examples

This example configures the prune wait time to 0 seconds.

```
device(config)# router pim
device(config-pim-router)# prune-wait 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# pw-profile

Creates a pseudowire (PW) profile that can be shared across multiple Virtual Private LAN Services (VPLS) bridge domains.

## Syntax

```
pw-profile [pw-profile-name [ mtu mtu-value ] [ mtu-enforce { false | true } ] [ vc-mode { raw | raw-passthrough | tag } ]
no pw-profile pw-profile-name [ mtu ] [ mtu-enforce ] [ vc-mode ] ]
```

## Command Default

No PW profile is configured.

## Parameters

*pw-profile-name*

Specifies the name of a PW profile.

**mtu** *mtu-value*

Specifies the maximum transmission unit (MTU) for the PW profile. The range is from 64 through 15966.

**mtu-enforce**

Configures MTU enforcement check during PW signaling.

*false*

Enables the MTU enforcement check.

*true*

Disables the MTU enforcement check.

**vc-mode**

Configures the virtual connection (VC) mode for the profile:

**raw**

Specifies using raw mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the VLAN tag is removed before it is sent out on the wire. When an untagged packet is received on an untagged AC endpoint it is encapsulated as is and sent out on the wire.

**raw-passthrough**

Specifies using raw-passthrough mode which enables interoperability with third-party devices. When all endpoints are configured as tagged endpoints, raw passthrough mode behaves the same way as tagged mode. When all endpoints are configured as untagged endpoints, raw-passthrough mode behaves the same way as raw mode. Select the **raw-passthrough** option, when all endpoints are configured as untagged endpoints (even when peer devices signal the PW VC mode as raw).

**tag**

Specifies using tag mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the packet is encapsulated as is and sent out on the wire. When an untagged packet is received on an untagged AC endpoint, a dummy tag is added and it is sent out on the wire.

## Modes

Global configuration mode.

## Usage Guidelines

You can configure up to 64 PW profiles.

The **no** form of the command removes the PW profile configuration.

## Examples

The following example shows how to create a PW profile named test specifying that the VC mode for the profile is raw-passthrough.

```
device# configure terminal
device(config)# pw-profile test vc-mode raw-passthrough
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# pw-profile (bridge domain)

Configures a pseudowire (PW) profile for a bridge domain.

## Syntax

**pw-profile** *pw-profile-name*

**no pw-profile**

## Command Default

A PW profile is not configured.

## Parameters

*pw-profile-name*

Specifies the name of the PW profile to attach to the bridge profile.

## Modes

Bridge-domain configuration mode.

## Usage Guidelines

The **no** form of the command removes the PW profile from the bridge-domain configuration.

## Examples

The following example shows how to configure a PW profile named test for bridge domain 1.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# pw-profile test
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# python

Launches an interactive Python shell, with an option to launch a Python script.

## Syntax

```
python [ python-statement | python-script-filename ]
```

## Parameters

*python-statement*

Must be a valid python interpreter argument.

*python-script-filename*

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

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is available only to users with admin-level permissions.

Entering **python**—with no additional parameters—launches an interactive Python shell.

Entering **python** *python-statement* launches an interactive Python shell and runs a valid *python-statement* that you enter. For example, entering `python -h` invokes the Python shell and displays Python options and arguments.

Entering **python** *python-script-filename* launches an interactive Python shell and runs the Python file. (To make a Python file available to this command, copy the Python file to the `flash://` location on the device, using the **copy** command.)

Note the following divergence between SLX-OS CLI syntax and Python syntax:

- Although in general, SLX-OS CLI syntax is not case-sensitive, Extreme convention is to use lower-case.
- Python syntax is case sensitive.

To exit the Python environment and return to the CLI, enter either:

- **exit()**
- **Ctrl-D**

## Examples

The following example launches the Python shell and then both assigns an SLX CLI operational command to a Python variable and runs that command.

```
device# python
Python 3.4.3 (default, Apr 11 2014, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_users = CLI('show users')
!Command: show users
!Time: Tue Aug 9 09:09:39 2016

**USER SESSIONS**
Username          Role      Host IP      Device  Time Logged In
jdoe              admin    10.11.12.13  Cli    2016-08-09 09:06:46
admin            admin    127.1.0.1    Cli    18640
**LOCKED USERS**
Username
no locked users
>>>
```

The following example (partial) launches the Python shell to run a Python script-file.

#### NOTE

For an annotated text of this script, refer to the *Extreme SLX-OS Management Configuration Guide* > "Python Event-Management and Scripting" > "Python scripts and run-logs."

```

device# python create_po.py
!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan dot1q tag native

!Command: config
vlan 101-105
!Time: Mon Aug 22 18:33:03 2016

!Command: show running-config vlan
!Time: Mon Aug 22 18:33:03 2016

vlan 1
!
vlan 101
!
vlan 102
!
vlan 103
!
vlan 104
!
vlan 105
!
vlan dot1q tag native

!Command: show running-config int po
!Time: Mon Aug 22 18:33:03 2016

interface Port-channel 1
description Insight port-channel on MM1
shutdown
!
interface Port-channel 2
description Insight port-channel on MM2
shutdown
!

!Command: config
int po 10
switchport
switchport mode trunk
switchport trunk allowed vlan add 101-105
switchport trunk tag native-vlan ; no shut
!Time: Mon Aug 22 18:33:03 2016

!Command: show running-config int po
!Time: Mon Aug 22 18:33:04 2016

interface Port-channel 1
description Insight port-channel on MM1
shutdown
!
interface Port-channel 2
description Insight port-channel on MM2
shutdown
!
interface Port-channel 10
switchport
switchport mode trunk

```

```

switchport trunk allowed vlan add 101-105
switchport trunk tag native-vlan
no shutdown
!

!Command: config
int eth 1/40
channel-group 10 mode active type standard
no shut
!Time: Mon Aug 22 18:33:04 2016

!Command: show running-config int eth 1/40
!Time: Mon Aug 22 18:33:04 2016

interface Ethernet 1/40
channel-group 10 mode active type standard
lACP timeout long
no shutdown
!

!Command: config
int eth 1/41
channel-group 10 mode active type standard
no shut
!Time: Mon Aug 22 18:33:04 2016

!Command: show running-config int eth 1/41
!Time: Mon Aug 22 18:33:05 2016

interface Ethernet 1/41
channel-group 10 mode active type standard
lACP timeout long
no shutdown
!

!Command: config
int eth 1/42
channel-group 10 mode active type standard
no shut
!Time: Mon Aug 22 18:33:05 2016

<output truncated>

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos cos

Changes the interface default Class of Service (CoS) value.

## Syntax

```
qos cos cos_value
```

## Command Default

The default is 0.

## Parameters

*value*

Specifies the CoS value. Valid values range from 0 through 7.

## Modes

Interface configuration mode

## Examples

To set the CoS value to 2 on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-fo-1/3)# qos cos 2
```

To set the CoS value to 2 on a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos cos-mutation

Applies a user configured QoS CoS-to-CoS mutation map to an interface.

## Syntax

```
qos cos-mutation cos_map_name
```

## Command Default

No explicit QoS CoS-to-CoS mutation map is applied; the inbound CoS equals the outbound CoS.

## Parameters

*cos\_map\_name*

The name of the CoS mutation map.

## Modes

Interface configuration mode

## Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

## Examples

Follow this example to apply a QoS CoS-to-CoS mutation map to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(config-if-eth-1/3)# qos cos-mutation cos_mutation_map
```

To apply a QoS CoS-to-CoS mutation map to a specific port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos-mutation cos_mutation_map
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos cos-traffic-class

Applies a Quality of Service (QoS) CoS-to-traffic class mutation map on an interface.

## Syntax

```
qos cos-traffic-class cos_map_name
```

## Command Default

No explicit QoS CoS-to-traffic class mutation map is applied; the inbound CoS equals the outbound CoS.

## Parameters

*cos\_tc\_map\_name*

The name of the CoS-to-traffic class mutation map.

## Modes

Interface configuration mode.

## Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

## Examples

To activate a QoS CoS-to-traffic class mutation map named `cosMutMap` on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(config-if-eth-1/3)# qos cos-mutation cosMutMap
```

To activate a QoS CoS-to-traffic class mutation map from a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos-mutation cosMutMap
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# qos cpu slot

Use this command to configure the traffic manager (TM) CPU port shaper rate (all towers) to the line card (LC) CPU.

## Syntax

```
qos cpu slot slot_id { group group_id { prio { priority | all } | shaper rate shaper_rate burst burst_size | wfq weight
weight_value }
qos cpu slot slot_id { port shaper rate shaper_rate burst burst_size }
no qos cpu slot slot_id { group group_id { prio { priority | all } | shaper rate shaper_rate burst burst_size | wfq weight
weight_value }
no qos cpu slot slot_id { port shaper rate shaper_rate burst burst_size }
```

## Command Default

The TM CPU group or port shaper rate is not set.

## Parameters

*slot\_id*

The slot values are 0 on Pizzabox platforms, 1 through 4 on F4 platforms and, 1 through 8 on F8 platforms.

**group** *group\_id*

Configures a CPU group.

**shaper rate** *shaper\_rate*

Configures the TM CPU shaper rate (all towers) to LC CPU for CPU groups. The rate is in kilo bits per second (Kbps) with a range from 0 through 100000.

**prio** *priority*

C onfigures the TM CPU shaper rate (all towers) to line card CPU for individual priority VoQs within a CPU group. The priority value ranges from 0 through 7.

**burst** *burst\_size*

Configures the CPU burst size. he burst size value has a a range from 1 through 64 KB.

**wfq weight** *weight\_value*

Configures the CPU group's weighted fair queue value (all towers). The weight value ranges from 1 through 128. Higher value.

**port**

Configures a CPU port.

## Modes

Global configuration mode.

## Usage Guidelines

The **no** form of the command removes the QoS CPU shaper configuration.

## Examples

Set the TM CPU port shaper on slot 1 to priority 5, rate of 4500 Kbps, and a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 port shaper rate 4000 burst 1
```

Set the TM CPU port shaper on slot 1 to 4000 Kbps w/ a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 port shaper rate 4000 burst 1
```

Set the TM CPU on slot 1 group 1 priority to 5, shaper to 4500 Kbps, and a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 group 1 priority 5 shaper rate 4500 burst 1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos dscp-cos

Applies a user configured QoS DSCP-to-CoS mutation map to an interface.

## Syntax

```
qos dscp-cos dscp_cos_map_name
```

## Command Default

No explicit QoS DSCP-to-CoS mutation map is applied.

## Parameters

*dscp\_cos\_map\_name*  
Name of DSCP-to-COS mutation map

## Modes

Interface configuration mode.

## Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

## Examples

Follow this example to apply a user configured QoS DSCP-to-COS mutation map named `dscpMap` to a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/2
device(config-if-eth-2/2)# qos dscp-cos dscpMap
```

Follow this example to apply a user configured QoS DSCP-to-COS mutation map named `dscpMap` to a specific port channel interface.

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-cos dscpMap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos dscp-mutation

Applies a user configured QoS DSCP mutation map to an interface.

## Syntax

```
qos dscp-mutation dscp_map_name
```

## Command Default

No explicit user configured QoS DSCP-to-DSCP mutation map is applied; the inbound DSCP equals the outbound DSCP.

## Parameters

*dscp\_map\_name*  
The name of the DSCP mutation map

## Modes

Interface subtype configuration mode

## Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

## Examples

Follow this example to apply a QoS DSCP-to-DSCP mutation map to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(config-if-eth-1/3)# qos dscp-mutation dscp_mutation_map
```

To apply a QoS DSCP-to-DSCP mutation map to a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-mutation dscp_mutation_map
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos dscp-traffic-class

Applies a user configured QoS DSCP-to-traffic- class mutation map to an interface.

## Syntax

```
qos dscp-traffic-class dscp_tc_name
```

## Command Default

No explicit user configured QoS DSCP-to-traffic class map is enabled on the interface.

## Parameters

*dscp\_tc\_name*  
Name of DSCP-to-traffic class map

## Modes

Interface configuration mode

## Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

## Examples

Follow this example to apply a QoS DSCP-to-traffic class mutation map to a specific 40-gigabit Ethernet interface

```
device# configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# qos dscp-traffic-class dscp_tc_map
```

Follow this example to apply a QoS DSCP-to-traffic class mutation map to a specific port channel interface

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-traffic-class dscp_tc_map
```

# qos map cos-mutation

Creates a QoS map for performing CoS-to-CoS mutation.

## Syntax

```
qos map cos-mutation name cos0 cos1 cos2 cos3 cos4 cos5 cos6 cos7
no qos map cos-mutation name
```

## Command Default

No CoS-to-CoS mutation QoS maps are defined.

## Parameters

*name*

Specifies a unique name across all CoS-to-CoS mutation QoS maps defined within the system. If the named CoS-to-CoS mutation QoS map does not exist, then it is created. If the named CoS-to-CoS mutation QoS map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the QoS map.

*cos#*

Specifies the outbound CoS value.

CoS value	Description
<i>cos0</i>	Sets the outbound CoS value for all packets with inbound CoS 0.
<i>cos1</i>	Sets the outbound CoS value for all packets with inbound CoS 1.
<i>cos2</i>	Sets the outbound CoS value for all packets with inbound CoS 2.
<i>cos3</i>	Sets the outbound CoS value for all packets with inbound CoS 3.
<i>cos4</i>	Sets the outbound CoS value for all packets with inbound CoS 4.
<i>cos5</i>	Sets the outbound CoS value for all packets with inbound CoS 5.
<i>cos6</i>	Sets the outbound CoS value for all packets with inbound CoS 6.
<i>cos7</i>	Sets the outbound CoS value for all packets with inbound CoS 7.

## Modes

Global configuration mode

## Usage Guidelines

A CoS-to-CoS mutation takes an inbound CoS value and maps it to an outbound CoS value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied. The outbound CoS value is used in selecting Traffic Class and egress packet marking.

Enter **no qos map cos-mutation name** command to delete the named CoS-to-CoS mutation QoS map. A QoS map can only be deleted if it is not bound to any interface.

## Examples

To create a CoS-to-CoS QoS mutation map to swap CoS 4 and CoS 5 and apply it on an interface, for example having inbound CoS 4 mapped to outbound CoS 5 and inbound CoS 5 mapped to outbound CoS 4; but all other CoS values go through unchanged:

```
device# configure terminal
device(config)# qos map cos-mutation cosMap 0 1 2 3 5 4 6 7
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# qos cos-mutation cosMap
```

To delete a CoS-to-CoS QoS mutation map:

```
device# configure terminal
device(config)# no qos map cos-mutation cosMap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos map cos-traffic-class

A QoS CoS-to-traffic class mutation map can be configured using the following command syntax

## Syntax

```
qos map cos-traffic-class name
no qos map cos-traffic-class name
```

## Command Default

If CoS-to-traffic class mutation map is not defined, the default CoS-to-traffic class map is used, which is a one-to-one map for each priority.

## Parameters

*name*

Specifies a unique name for the CoS-to-traffic class mutation QoS map. If the named map does not exist, then it is created. If the map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the map.

## Modes

Global configuration mode

## Usage Guidelines

A CoS-to-traffic class mutation map takes an inbound CoS value and maps it to an outbound traffic class (priority queue) value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied.

The drop-precedence parameter is optional.

Enter **no qos map cos-traffic-class *name*** command to delete the named QoS CoS-to-traffic class mutation map.

A QoS map can only be deleted if it is not bound to an interface.

## Examples

To create a QoS CoS-to-traffic class mutation map use the following command

```
device# configure terminal
device(config)# qos map cos-traffic-class cosTC1
device(cos-traffic-class-cosTC1)# map cos 4 to traffic-class 3 drop-precedence 0
device(cos-traffic-class-cosTC1)# map cos 5 to traffic-class 5 drop-precedence 1
device(cos-traffic-class-cosTC1)# map cos 6 to traffic-class 6 drop-precedence 0
device(cos-traffic-class-cosTC1)# map cos 7 to traffic-class 6 drop-precedence 1
device(cos-traffic-class-cosTC1)# interface ethernet 1/1
device(conf-if-eth-1/1)# qos cos-traffic-class cosTC1
```



To delete a QoS CoS-to-traffic class mutation map that is bound to an interface follow this example.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no qos cos-traffic-class cosTC1
device(conf-if-eth-1/1)# exit
device(config)# no qos map cos-traffic-class cosTC1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## qos map dscp-cos

Creates a QoS map where the ingress DSCP value is mapped to outgoing 802.1P values. This configures a DSCP-to-CoS map on the ingress interface.

### Syntax

```
qos map dscp-cos name
no qos map dscp-cos name
map dscp ingress dscp values to cos cos
```

### Command Default

DSCP-to-CoS mutation is not enabled.

### Parameters

*name*  
Name of DSCP-to-CoS map

**map dscp**  
Ingress DSCP values.

**cos**  
Egress CoS values.

*ingress dscp values*  
Input DSCP values. The range of ingress DSCP values is 0 through 63.

*cos*  
CoS value. The range is 0 through 7.

### Modes

dscp-cos mode for the QoS **map dscp** commands  
Global configuration mode

### Usage Guidelines

This command remaps the incoming DSCP values of the ingress packet to egress CoS 802.1P values.

When you enter **qos map dscp-cos**, the system is placed in dscp-cos mode for the configured map. At this point, you can map ingress DSCP values to egress CoS values using the **map dscp** command.

Enter **qos dscp-cos name** while in configuration mode for a specific interface to apply the DSCP-to-CoS map to that interface.

Enter **no qos dscp-cos name** while in the interface configuration mode to remove the DSCP-to-CoS map from the interface.

Enter **no map dscp-cos name** while in global configuration mode to remove the DSCP-to-CoS map.

## Examples

To create a QoS DSCP-to-CoS map and place system into dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)#
```

To map an ingress DSCP value to egress CoS value while in dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
```

To map multiple ingress DSCP values to egress CoS values while in dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
device(dscp-cos-test)# map dscp 63 to cos 6
device(dscp-cos-test)# map dscp 53 to cos 5
device(dscp-cos-test)# map dscp 23 to cos 2
```

To remove a QoS DSCP-CoS map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-cos test
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos map dscp-mutation

Creates a DSCP mutation by mapping the incoming DSCP value of the ingress packet to outgoing DSCP values.

## Syntax

**qos map dscp-mutation** *name*

**no map qos dscp-mutation** *name*

**map dscp** *ingress dscp values to dscp egress dscp value*

## Command Default

DSCP mutation is not enabled.

## Parameters

*name*

Name of DSCP mutation map

**map dscp**

Inbound DSCP values.

*ingress dscp values*

The ingress DSCP values. The range is from 0 through 63.

**dscp**

Outbound DSCP values.

*egress dscp values*

The egress DSCP value. The range is from 0 through 63.

## Modes

dscp-mutation mode for the DSCP mutation map

Global configuration mode

## Usage Guidelines

Enter **qos dscp-mutation** *name* while in configuration mode for a specific interface to apply the DSCP mutation map to that interface. When you enter **qos map dscp-mutation**, the system is placed in dscp-mutation mode for the configured map. At this point, you can map ingress DSCP values to egress DSCP values using the **dscp map** command.

Enter **no qos dscp-mutation** *name* while in interface configuration mode to remove the DSCP mutation map from that interface.

Enter **no map dscp-mutation** *name* while in global configuration mode to remove the DSCP mutation map.

## Examples

To create a QoS DSCP mutation map and place system into dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)#
```

To map an ingress DSCP value to egress DSCP values while in dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 1,3,5,7 to dscp 40
```

To map multiple ingress DSCP values to egress DSCP values while in dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 60 to dscp 40
device(dscp-mutation-test)# map dscp 24 to dscp 50
device(dscp-mutation-test)# map dscp 33 to dscp 35
device(dscp-mutation-test)# map dscp 53 to dscp 61
```

To remove a QoS DSCP mutation map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-mutation test
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos map dscp-traffic-class

Creates a QoS map for performing DSCP-to-traffic class mapping. This creates a DSCP-to-traffic class map on the ingress interface. You can configure an interface with either a DSCP-to-traffic class map or a CoS-to-traffic class map.

## Syntax

```
qos map dscp-traffic-class name
```

```
no qos map dscp-traffic-class name
```

```
map dscp ingress dscp values to traffic-class traffic class [ drop-precedence out drop precedence ]
```

## Command Default

DSCP-to-traffic class mutation is not enabled.

## Parameters

*name*

Name of the QoS DSCP-to-traffic clas map.

**map dscp**

Ingress DSCP values. The range of ingress DSCP values is 0 through 63.

**traffic-class**

Egress traffic class values. The range of ingress traffic class values is from 0 through 7.

**drop-precedence**

Drop precedence value given egress packets. The range is 0 through 3.

*ingress dscp values*

Range of input DSCP values. The range is 0 through 63.

*traffic class*

The traffic class value. the range is from 0 through 7.

*out drop precedence*

Value of the output drop precedence. The range is 0 through 3.

## Modes

dscp-traffic-class mode for the DSCP-to-traffic class map

Global configuration mode

## Usage Guidelines

Enter **qos dscp-traffic-class** *name* while in configuration mode for a specific interface to apply the QoS DSCP-Traffic-Class map to that interface. When you enter **qos map dscp-traffic-class**, the system is placed in dscp-traffic-class mode for the configured map. At this point, you can map ingress DSCP values to traffic class values using the **mark** command.

Enter **no qos dscp-traffic-class** *name* while in the interface mode to remove the map from that interface.

## Examples

To create a QoS DSCP-to-traffic class map and place system into dscp-traffic-class mode:

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)#
```

To map ingress DSCP values to a traffic class while in dscp-traffic-class mode:

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 1,3,5,7 to traffic-class 1 drop-precedence 1
```

To map multiple ingress DSCP values to traffic classes and drop precedence while in dscp-traffic-class mode:

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 10 to traffic-class 3 drop-precedence 1
device(dscp-traffic-class-test)# map dscp 40 to traffic-class 4 drop-precedence 1
device(dscp-traffic-class-test)# map dscp 45 to traffic-class 5 drop-precedence 0
device(dscp-traffic-class-test)# map dscp 52 to traffic-class 3 drop-precedence 1
```

To remove a QoS DSCP-traffic class map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-traffic-class test
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos map traffic-class-cos

A QoS traffic class-to-CoS mutation map can be configured to create a priority mapping table using a traffic-class-cos map. The traffic class-to-CoS map is then applied to an egress interface to effect the priority re-mapping.

## Syntax

```
qos map traffic-class-cos name
no qos map traffic-class-cos name
```

## Command Default

If a QoS traffic class-to-CoS mutation map is not defined, the default traffic class-to-CoS map is used, which is a one-to-one map for each priority.

## Parameters

*name*

Specifies a unique name for the QoS traffic class-to-CoS mutation map. If the named map does not exist, then it is created. If the map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the map.

## Modes

Global configuration mode

## Usage Guidelines

A traffic class can be mapped to the outgoing PCP value when a packet egresses the switch. You can create a priority mapping table using a traffic class-to-CoS map. This traffic class-to-CoS map can then be applied to an egress interface to effect the priority re-mapping. This feature only maps the internal traffic class to outgoing priority.

Enter **no qos map traffic-class-cos name** command to delete the named QoS traffic class-to-CoS mutation map.

A QoS map can only be deleted if it is not bound to an interface.

## Examples

To create and apply a QoS traffic class-to-CoS mutation map use the following command:

```
device# configure terminal
device(config)# qos map traffic-class-cos CoSMap
device(traffic-class-cos-CoSMap)# map traffic-class 3 drop-precedence 1 to cos 2
device(traffic-class-cos-CoSMap)# map traffic-class 4 drop-precedence 1 to cos 3
device(traffic-class-cos-CoSMap)# map traffic-class 5 drop-precedence 2 to cos 4
device(conf-if-eth-1/4)# qos traffic-class-cos tcCos1
```



To delete a QoS traffic class-to-CoS mutation map that is bound to an interface follow this example.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# no qos traffic-class-cos CoSMap
device(conf-if-eth-1/4)# exit
device(config)# no qos map traffic-class-cos CoSMap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map dscp-exp

Creates and populates an MPLS QoS differentiated services code point (DSCP) to EXP mutation map.

## Syntax

```
qos-mpls map dscp-exp mapname { dscp dscp_value to exp exp_value }
[no] qos-mpls map dscp-exp mapname [ dscp dscp_value to exp exp_value ]
```

## Parameters

*mapname*

The name of the MPLS QoS DSCP-to-EXP mutation map. The name can be up to 64 characters.

**dscp**

Specifies that the ingress DSCP value follows.

*dscp\_value*

The ingress DSCP value. The range is from 0 through 63.

**exp**

Specifies that the egress EXP value follows.

*exp\_value*

The egress EXP value. The range is from 0 through 7.

## Modes

Global configuration mode

dscp-exp-mapname configuration mode

## Usage Guidelines

Creating the map and setting the initial mutation places the device into `dscp-exp-mapname` configuration mode where you continue to populate the map using the **dscp** command.

MAC filter and DSCP marking cannot be configured on the same port.

## Examples

Follow this example to create an MPLS QoS DSCP-to-EXP mutation map.

```
device# configure terminal
device(config)# qos-mpls map dscp-exp dscpExpMap dscp 0 to exp 1
device(dscp-exp-dscpExpMap)# dscp 3 to exp 2
device(dscp-exp-dscpExpMap)# dscp 17 to exp 4
device(dscp-exp-dscpExpMap)# dscp 61 to exp 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map exp-dscp

Creates and populates an MPLS QoS EXP to differentiated services code point (DSCP) mutation map.

## Syntax

```
qos-mpls map exp-dscp mapname { exp exp_value to dscp dscp_value }
[no] qos-mpls map exp-dscp mapname [ exp exp_value to dscp dscp_value ]
```

## Parameters

*mapname*

The name of the MPLS QoS EXP-to\_DSCP mutation map. The name can be up to 64 characters.

**exp**

Specifies that the egress EXP value follows.

*exp\_value*

The ingress EXP value. The range is from 0 through 7.

**dscp**

Specifies that the egress DSCP value follows.

*dscp\_value*

The egress DSCP value. The range is from 0 through 63.

## Modes

Global configuration mode

exp-dscp-mapname configuration mode

## Usage Guidelines

Creating the map and setting the initial mutation places the device into exp-dscp-mapname configuration mode where you continue to populate the map using the **exp** command.

## Examples

Follow this example to create an MPLS QoS EXP-to-DSCP mutation map.

```
device# configure terminal
device(config)# qos-mpls map exp-dscp expDscpMap exp 1 to dscp 2
device(exp-dscp-expDscpMap)# exp 2 to dscp 4
device(exp-dscp-expDscpMap)# exp 4 to dscp 8
device(exp-dscp-expDscpMap)# exp 6 to dscp 12
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map exp-traffic-class

Creates and populates an MPLS QoS EXP to traffic class mutation map.

## Syntax

```
qos-mpls map exp-traffic-class mapname { exp exp_value to traffic-class traffic_class_value drop-precedence
drop_precedence_value }
```

```
[no] qos-mpls map exp-traffic-class mapname [ exp exp_value to traffic-class traffic_class_value drop-precedence
drop_precedence_value ]
```

## Parameters

*mapname*

The name of the MPLS QoS EXP-to-traffic class mutation map. The name can be up to 64 characters.

**exp**

Specifies that the egress EXP value follows.

*exp\_value*

The ingress EXP value. The range is from 0 through 7.

**traffic-class**

Specifies that the egress traffic class value follows.

*traffic\_class\_value*

The egress traffic class value. The range is from 0 through 63.

**drop-precedence**

Specifies that the traffic class drop precedence value follows.

*drop\_precedence\_value*

The egress traffic class drop precedence value. The range is from 0 through 3.

## Modes

Global configuration mode

exp-traffic-class-mapname configuration mode

## Usage Guidelines

Creating the map and setting the initial mutation places the device into `exp-traffic-class-mapname` configuration mode where you continue to populate the map using the **exp** command.

## Examples

Follow this example to create an MPLS QoS EXP-to-traffic class mutation map.

```
device# configure terminal
device(config)# qos-mpls map exp-traffic-class expTCMap exp 1 to traffic-class 2 drop-precedence 2
device(exp-traffic-class-expTCMap)# exp 2 to traffic-class 4 drop-precedence 2
device(exp-traffic-class-expTCMap)# exp 4 to traffic-class 8 drop-precedence 2
device(exp-traffic-class-expTCMap)# exp 6 to traffic-class 12 drop-precedence 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map traffic-class-exp

Creates and populates an MPLS QoS traffic class-to-EXP mutation map.

## Syntax

```
qos-mpls map traffic-class-exp mapname { traffic-class traffic_class_value drop-precedence drop_precedence_value to exp exp_value }
```

```
[no] qos-mpls map traffic-class-exp mapname [ traffic-class traffic_class_value drop-precedence drop_precedence_value to exp exp_value ]
```

## Parameters

*mapname*

The name of the MPLS QoS traffic class-to-EXP mutation map. The name can be up to 64 characters.

**traffic-class**

Specifies that the ingress traffic class value follows.

*traffic\_class\_value*

The ingress traffic class value. The range is from 0 through 63.

**drop-precedence**

Specifies that the traffic class drop precedence value follows.

*drop\_precedence\_value*

The egress traffic class drop precedence value. The range is from 0 through 3.

**exp**

Specifies that the egress EXP value follows.

*exp\_value*

The egress EXP value. The range is from 0 through 7.

## Modes

Global configuration mode

`traffic-class-exp-mapname` configuration mode

## Usage Guidelines

Creating the map and setting the initial mutation places the device into `traffic-class-exp-mapname` configuration mode where you continue to populate the map using the **traffic-class** command.



## Examples

Follow this example to create an MPLS QoS traffic class-to-EXP mutation map.

```
device# configure terminal
device(config)# qos-mpls map traffic-class-exp tcExpMap traffic-class 0 drop-precedence 2 to exp 1
device(traffic-class-exp-tcExpMap)# traffic-class 3 drop-precedence 2 to exp 4
device(traffic-class-exp-tcExpMap)# traffic-class 4 drop-precedence 2 to exp 5
device(traffic-class-exp-tcExpMap)# traffic-class 5 drop-precedence 2 to exp 6
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map-apply dscp-exp

Applies an MPLS DSCP to EXP mutation map globally.

## Syntax

```
qos-mpls map-apply dscp-exp { map_name | all-zero-map | default-map } { all }
[no] qos-mpls map-apply dscp-exp
```

## Parameters

*map\_name*

The name of the user-defined map that you are applying.

**all-zero-map**

Maps the DSCP values to EXP 0.

**default-map**

Maps the DSCP to EXP values based on the default map.

**all**

Applies the map globally.

## Modes

Global configuration mode

## Examples

Follow this example to apply a MPLS DSCP to EXP mutation map.

```
device# configure terminal
device(config)# qos-mpls map-apply dscp-exp dscpExpMap all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map-apply exp-dscp

Applies an MPLS EXP to DSCP mutation map globally.

## Syntax

```
qos-mpls map-apply exp-dscp { map_name | all-zero-map | default-map } { all }
[no] qos-mpls map-apply exp-dscp
```

## Parameters

- map\_name*  
The name of the user-defined map that you are applying.
- all-zero-map**  
Maps the EXP values to DSCP 0.
- default-map**  
The EXP to DSCP value is based on the default map.
- all**  
Applies the map globally.

## Modes

Global configuration mode

## Examples

Follow this example to apply a MPLS EXP to DSCP mutation map.

```
device# configure terminal
device(config)# qos-mpls map-apply exp-dscp expDscppMap all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map-apply exp-traffic-class

Applies an MPLS EXP to traffic class mutation map globally.

## Syntax

```
qos-mpls map-apply exp-traffic-class { map_name | all-zero-map | default-map } { all }
[no] qos-mpls map-apply exp-traffic-class
```

## Parameters

*map\_name*

The name of the user-defined map that you are applying.

**all-zero-map**

Maps the EXP values to internal traffic class 0 and drop precedence 0.

**default-map**

Maps the EXP to internal traffic class values and drop precedence based on the default map.

**all**

Applies the map globally.

## Modes

Global configuration mode

## Examples

Follow this example to apply a MPLS EXP to traffic class mutation map.

```
device# configure terminal
device(config)# qos-mpls map-apply exp-traffic-class expTrafficClassMap all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos-mpls map-apply traffic-class-exp

Applies an MPLS traffic class mutation to EXP map globally.

## Syntax

```
qos-mpls map-apply traffic-class-exp { map_name | all-zero-map | default-map } { all }
[no] qos-mpls map-apply traffic-class-exp
```

## Parameters

*map\_name*

The name of the user-defined map that you are applying.

**all-zero-map**

Maps the internal traffic class and drop precedence values to EXP 0.

**default-map**

Maps the internal traffic class and drop precedence values to EXP based on the default map.

**all**

Applies the map globally.

## Modes

Global configuration mode

## Examples

Follow this example to apply a MPLS traffic class to EXP mutation map.

```
device# configure terminal
device(config)# qos-mpls map-apply traffic-class-exp trafficClassExpMap all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos rx-queue cos-threshold

Configures the QoS ingress queue cost of service (CoS) thresholds.

## Syntax

```
qos rx-queue cos-threshold threshold_value_0 threshold_value_1 threshold_value_2 threshold_value_3 threshold_value_4
threshold_value_5 threshold_value_6 threshold_value_7
```

```
[no] qos rx-queue cos-threshold
```

## Command Default

The CoS threshold values for the ingress queue are not configured.

## Parameters

*threshold\_value\_n*

There are eight entries for this parameter with each entry representing a percentage. Each position matches a specific inbound CoS with the first position (**cos\_threshold\_0**) representing CoS 0, the second CoS 1, and so on.

## Modes

Ethernet interface configuration mode.

## Usage Guidelines

The total of all the entries cannot exceed 100%.

A 0 may be entered for any of the values.

## Examples

Follow this example to configure the QoS ingress queue CoS thresholds on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# qos rx-queue cos-threshold 10 10 10 10 10 20 20 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos rx-queue multicast best-effort-rate

Configures the multicast packet best effort rate limit parameter on an Ethernet interface.

## Syntax

```
qos rx-queue multicast best-effort-rate best-_effort_rate
```

```
[no] qos rx-queue multicast best-effort-rate
```

## Command Default

There best effort rate limiting parameter is not set for the multicast ingress queue.

## Parameters

*best\_effort\_rate*

The best effort rate on the multicast ingress queue. The rate ranges from 0 to 600000000 kilo bits per second.

## Modes

Ethernet interface configuration mode

## Examples

Follow this example to set an Ethernet interface multicast ingress queue best effort rate limit.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# qos rx-queue multicast best-effort-rate 500000000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos rx-queue multicast guarantee-rate

Configures the multicast packet guaranteed rate limit parameter on an Ethernet interface.

## Syntax

```
qos rx-queue multicast guarantee-rate guarantee_rate
```

```
[no] qos rx-queue multicast guarantee-rate
```

## Command Default

There are guaranteed rate limit parameter is notset for the multicast ingress queue.

## Parameters

*guarantee\_rate*

The guaranteed rate on the multicast ingress quque. The rate ranges from 0 to 600000000 kilo bits per second.

## Modes

Ethernet interface configuration mode

## Examples

Follow this example to set an Ethernet interface receive queue guaranteed rate.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# qos rx-queue multicast guarantee-rate 450000000
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# qos rx-queue multicast traffic-class

Configures the ingress queue multicast packet traffic class parameter on an Ethernet interface.

## Syntax

```
qos rx-queue multicast traffic-class traffic_class min-queue-size minimum_size max-queue-size maximum_size
[no] qos rx-queue multicast traffic-class
```

## Command Default

There are no traffic class parameters set for the multicast ingress queue.

## Parameters

*traffic\_class*

The traffic class, the value ranges from 0 to 7.

**min-queue-size**

Sets the multicast ingress queue minimum size.

*minimum\_size*

The minimum size of the multicast ingress queue. The size value ranges from 0 through 1025 KB

**max-queue-size**

Sets the multicast ingress queue minimum size.

*maximum\_size*

The minimum size of the multicast ingress queue. The size value ranges from 0 through 6124 MB.

## Modes

Ethernet interface configuration mode

## Examples

Follow this example to set an Ethernet interface ingress queue minimum and maximum queue size by a traffic class.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# qos rx-queue multicast traffic-class 4 min-queue-size 512 max-queue-size 3071
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos rx-queue unicast traffic-class

Configures the ingress queue unicast packet traffic class parameter on an Ethernet interface.

## Syntax

```
qos rx-queue unicast traffic-class traffic_class min-queue-size minimum_size max-queue-size maximum_size
[no] qos rx-queue unicast traffic-class
```

## Command Default

There are no traffic class parameters set for the unicast ingress queue.

## Parameters

*traffic\_class*

The traffic class, the value ranges from 0 to 7.

**min-queue-size**

Sets the unicast ingress queue minimum size.

*minimum\_size*

The minimum size of the unicast ingress queue. The size value ranges from 0 through 1025 KB

**max-queue-size**

Sets the unicast ingress queue minimum size.

*maximum\_size*

The minimum size of the unicast ingress queue. The size value ranges from 0 through 6124 MB.

## Modes

Ethernet interface configuration mode

## Examples

Follow this example to set an Ethernet interface ingress queue minimum and maximum queue size by a traffic class.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# qos rx-queue unicast traffic-class 4 min-queue-size 512 max-queue-size 3071
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos service-policy

Applies a policy map to all inbound traffic.

## Syntax

```
qos service-policy in service_policy_name
```

```
no qos service-policy in service_policy_name
```

## Parameters

**in**

Applies the service policy to inbound traffic.

*service\_policy\_name*

The name of the policy map.

## Modes

Global configuration mode.

## Usage Guidelines

The policy map has been preconfigured.

Enter **no qos service-policy in *service\_policy\_name*** to return to the default.

## Examples

This example binds a service policy to inbound traffic at the system level.

```
device# configure terminal
device(config)# qos service-policy in policyMap1
device(config-service-policy-in/policyMap1)# end
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos traffic-class

Applies a QoS default traffic class value to an interface.

## Syntax

```
qos traffic-class default_tc_value
```

## Command Default

No explicit user configured QoS default traffic class priority value is configured.

## Parameters

*default\_tc\_value*

The assigned traffic class priority value. The traffic class priority values range from 0 through 7.

## Modes

Interface configuration mode

## Examples

Follow this example to apply a default traffic class value to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos traffic-class 3
```

Follow this example to apply a default traffic class value to a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos traffic-class 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos traffic-class-cos

Applies a user configured QoS traffic class-to-CoS mutation map to an interface.

## Syntax

```
qos traffic-class-cos tc_cos_map
```

## Command Default

No explicit user configured QoS traffic class-to-CoS mutation maps are applied. The outbound traffic class equals the inbound traffic class.

## Parameters

*tc\_cos\_map*

The name of the user configured QoS traffic class-to-CoS mutation map.

## Modes

Interface configuration mode.

## Usage Guidelines

The mutation maps are preconfigured.

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

## Examples

Follow this example to apply a user configured QoS traffic class-to-CoS mutation map to an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(config-if-eth-1/5)# qos traffic-class-cos tc_cos_map
```

Follow this example to apply a user configured QoS traffic class-to-CoS mutation map) to a port channel interface.

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos traffic-class-cos tc_cos_map
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# qos tx-queue scheduler strict-priority

Configures the strict priority (SP) value for the egress queue traffic class scheduler and assigns a deficit weighted round robin (DWRR) weight.

## Syntax

```
qos tx-queue scheduler strict-priority traffic_class dwrr dwrr_weight
```

```
[no] qos tx-queue scheduler strict-priority traffic_class dwrr dwrr_weight
```

## Command Default

The SP value for the egress queue traffic class scheduler is not configured.

## Parameters

*traffic\_class*

There are eight traffic class values:

Value	Traffic class
0	No strict priority queue.
1	Traffic class 7 strict priority queue.
2	Traffic class 6 through 7 strict priority queues.
3	Traffic class 5 through 7 strict priority queues.
4	Traffic class 4 through 7 strict priority queues.
5	Traffic class 3 through 7 strict priority queues.
6	Traffic class 2 through 7 strict priority queues.
7	Traffic class 1 through 7 strict priority queues.

*dwrr dwrr\_weight*

Configure the DWRR queue weights. There are eight entries for this parameter with each entry representing a percentage. The total of all the entries cannot exceed 100%. Each entry position represents a specific traffic class:

Place	Assignment
1	Traffic class 0 DWRR weight.
2	Traffic class 1 DWRR weight.
3	Traffic class 2 DWRR weight.
4	Traffic class 3 DWRR weight.
5	Traffic class 4 DWRR weight.
6	Traffic class 5 DWRR weight.
7	Traffic class 6 DWRR weight.
8	Traffic class 7 DWRR weight.

## Modes

Global configuration mode

## Usage Guidelines

The no form, of the command removes the SP value for the egress queue traffic class scheduler.

## Examples

Use the following command to assign traffic classes 6 through 7 to a SP queue and assign DWRR weights.

```
device# configure terminal
device(config)# qos tx-queue scheduler strict-priority 2 dwrr 20 5 5 5 20 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.





# Commands R - Sh

---

## radius-server

Configures the Remote Authentication Dial-In User Service (RADIUS) server.

### Syntax

```
radius-server host { ip-address | host_name } [ auth-port portnum ] [ protocol { chap | pap | peap-mschap } ] [ key shared_secret ] [ encryption-level value_level ] [ timeout sec ] [ retries num ] [ use-vrf vrf-name ]  
no radius-server host hostname | ip-address [ use-vrf vrf-name ]
```

### Command Default

A Remote Authentication Dial-In User Service (RADIUS) server is not configured.

### Parameters

**host** { *ipaddr* | *host\_name* }

Specifies the IP address or host name of the RADIUS server. IPv4 and IPv6 addresses are supported. The maximum supported length for the RADIUS hostname is 40 characters.

**auth-port** *portnum*

Specifies the user datagram protocol (UDP) port used to connect the RADIUS server for authentication. The valid range is 0 through 65535. The default port is 1812.

**protocol** { **chap** | **pap** | **peap-mschap** }

Specifies the authentication protocol. Parameters include CHAP, PAP, or PEAP-MSCHAP. The default is CHAP.

**key** *shared\_secret*

The text string that is used as the shared secret between the device and the RADIUS server. The default is **sharedsecret**. The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and you can specify the shared secret string in either double quotation marks or use the escape character (\). For example: **"secret!key"** or **secret\!key**.

**encryption-level** *value\_level*

Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The valid values are 0 and 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 7.

**timeout** *sec*

The time to wait for the RADIUS server to respond, in seconds. The default is 5 seconds.

**retries** *num*

The number of attempts allowed to connect to a RADIUS server. The default is 5 attempts.

**use-vrf** *vrf-name*

Specifies a VRF through which to communicate with the RADIUS server. See the Usage Guidelines.

## Modes

Global configuration mode

## Usage Guidelines

If a RADIUS server with the specified IP address or host name does not exist, it is added to the server list. If the RADIUS server already exists, this command modifies the configuration.

The **key** parameter does not support an empty string.

Enter **no radius-server** to reset to their default values.

### NOTE

Before downgrading to a software version that does not support the **encryption-level** keyword, set the value of this keyword to 0. Otherwise, the firmware download will throw an error that requests this value be set to 0.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

## Examples

To configure a RADIUS server:

```
device# configure terminal
device(config)# radius-server host 10.24.65.6
device(config-radius-server-10.24.65.6/mgmt-vrf)# protocol chap retransmit 100
device(config-host-10.24.65.6/mgmt-vrf)#
```

To modify the previously configured RADIUS server:

```
device(config)# radius-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# protocol pap key "new#radius*secret" timeout 10
```

To reset the timeout value to the default:

```
device# configure terminal
device(config)# no radius-server host 10.24.65.6 timeout
```

To communicate with the server through a user-specified VRF:

```
device# configure terminal
device(config)# radius-server host 10.24.65.6 use-vrf my-vrf
device(config-host-10.24.65.6/mgmt-vrf)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# reconnect-time

Specifies the amount of time that a graceful restart (GR) neighbor must wait for the LDP session to be reestablished.

## Syntax

**reconnect-time** *seconds*

**no reconnect-time** *seconds*

## Command Default

The default reconnect time is 120 seconds.

## Parameters

*seconds*

Specifies the amount of time in seconds that a GR neighbor must wait for the LDP session to be reestablished. This value is advertised to the neighbor using the FT Reconnect Timeout field in the FT Session TLV. Enter a integer from 60 to 300. The default setting is 120.

## Modes

MPLS LDP GR configuration mode

## Usage Guidelines

The **no** form of the command resets the default time of 120 seconds.

## Examples

The following example sets the LDP GR timer to 180 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# reconnect-time 180
```

## History

Release version	Command history
16r. 1.00	This command was introduced.

# recovery-time

Specifies the amount of time that this device retains its MPLS forwarding state across LDP graceful restart (GR).

## Syntax

**recovery-time** *seconds*

**no recovery-time** *seconds*

## Command Default

The default recovery time is 120 seconds.

## Parameters

*seconds*

Specifies the amount of time in seconds that this router retains its MPLS forwarding state across restart. This value is advertised to the neighbor using the Recovery Time field in the FT Session TLV. Enter a integer from 60 to 3600.

## Modes

MPLS LDP GR configuration mode

## Usage Guidelines

The recovery time must be chosen accordingly taking into account the time it takes for RTM to recompute the routes and the number of Layer 3 FECs that need to be recovered as part of the LDP GR recovery. This is applicable to GR processing on ingress as well as transit LSRs.

The **no** form of the command resets the default time of 120 seconds.

## Examples

The following example sets the LDP GR timer to 240 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# recovery-time 240
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# redistribute

Configures the device to redistribute IPv4 and IPv6 routes from one routing domain to another.

## Syntax

```
redistribute isis [ level-1 | level-1-2 | level-2 | metric num | route-map string ]
redistribute isis { level-1 into level-2 } [ prefix-list name ]
redistribute isis { level-2 into level-1 } [ prefix-list name ]
redistribute ospf [ match { external1 | external2 | internal } | metric num | metric-type { type1 | type2 } | route-map string ]
redistribute { source-protocol } [ metric num | metric-type { type1 | type2 } | route-map string ]
redistribute { source-protocol } [ level-1 | level-1-2 | level-2 | metric num | metric-type { type1 | type2 } | route-map string ]
no redistribute isis [ level-1 | level-1-2 | level-2 metric num | route-map string ]
no redistribute isis { level-1 into level-2 } [ prefix-list name ]
no redistribute isis { level-2 into level-1 } [ prefix-list name ]
no redistribute ospf [ match { external1 | external2 | internal } | metric num | metric-type { type1 | type2 } | route-map string ]
no redistribute { source-protocol } [ metric num | metric-type { type1 | type2 } | route-map string ]
```

## Command Default

The device does not redistribute routing information.

## Parameters

### isis

Specifies the ISIS protocol.

### level-1

Specifies L1 LSP, L1 CSNP and LI PSNP packets.

### level-1-2

Specifies both L1 LSP, L1 CSNP and LI PSNP packets and L2 LSP, L2 CSNP and L2 PSNP packets.

### level-2

Specifies L2 LSP, L2 CSNP and L2 PSNP packets.

### metric num

Specifies a metric for redistributed routes. Range is from 1 through 65535 in OSPFv2 and OSPFv3 configuration mode. Range is from 1 through 4261412863 in ISIS address-family IPv4/IPv6 unicast configuration mode and BGP address-family IPv4/IPv6 unicast configuration mode.

### route-map string

Specifies a route map to be consulted before a route is added to the routing table.

### level-1 into level-2

Redistributes Level 1 routes into Level 2.

**level-2 into level-1**

Redistributes Level 2 routes into Level 1.

**prefix-list** *name*

Specifies a prefix-list.

**ospf**

Specifies the OSPF protocol.

**match**

Specifies the type of route.

**external1**

Specifies OSPF Type 1 external routes.

**external2**

Specifies OSPF Type 2 external routes.

**internal**

Specifies OSPF internal routes.

**metric-type**

Specifies the external link type associated with the default route advertised into the OSPF routing domain.

**type1**

Specifies a type 1 external route.

**type2**

Specifies a type 2 external route.

*source-protocol*

Specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, or **static**.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

ISIS address-family IPv4 unicast configuration mode

ISIS address-family IPv6 unicast configuration mode

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

Routes can be filtered by means of an associated route map before they are distributed.

The **metric-type** { **type1** | **type2** } option is only available in OSPFv3 router, OSPFv3 router VRF, and ISIS address-family / IPv4/IPv6 unicast configuration mode.

The **redistribute** { *source-protocol* } [ **level-1** | **level-1-2** | **level-2** ] option is only available in ISIS address-family IPv4/IPv6 unicast configuration mode.

#### [ **match metric** **metric-type**

##### NOTE

The **default-metric** command does not apply to the redistribution of directly connected routes. Use a route map to change the default metric for directly connected routes.

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

## Examples

The following example redistributes IS-IS routes, specifying level 1 packets, in BGP address-family IPv4 unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# redistribute isis level-1
```

The following example redistributes all IPv4 IS-IS routes from Level 2 into Level 1.

```
device# configure terminal
device(config)# router isis
device(config-bgp-isis)# address-family ipv4 unicast
device(config-bgp-ipv4u)# redistribute isis level-2 into level-1
```

The following example redistributes OSPF external type 1 routes with a metric of 200 in BGP address-family IPv4 unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# redistribute ospf match external1 metric 200
```

The following example redistributes OSPFv3 external type 2 routes in BGP address-family IPv6 unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# redistribute ospf match external2
```

The following example redistributes static routes into BGP4 and specifies a metric of 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# redistribute static metric 200
```

The following example redistributes directly connected routes into BGP4+.

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

The following example redistributes directly connected routes into IS-IS.

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

The following example redistributes BGP routes and specifies that route-map "rm7" be consulted in OSPF VRF configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# redistribute bgp route-map rm7
```

The following example redistributes OSPF routes and specifies a type1 external route in OSPFv3 VRF configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# redistribute ospf metric-type type1
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# refresh-reduction

When the user enables either of the refresh reduction extensions on an interface, outgoing RSVP packets sent on that interface sets the refresh reduction capability bit in the common RSVP header to indicate that the device is capable of receiving and processing refresh reduction messages and related objects.

## Syntax

```
refresh-reduction bundle-message [ bundle-send-delay milliseconds ] | summary-refresh
no refresh-reduction bundle-message [ bundle-send-delay milliseconds ] | summary-refresh
```

## Command Default

The RSVP bundle messages on the interface are disabled, by default.

## Parameters

### bundle-message

#### bundle-send-delay *milliseconds*

Specifies the bundle send delay value in milliseconds. the range is 20-1000 milliseconds, with a default of 40 milliseconds.

#### summary-refresh

Activates the refresh-reduction summary refresh.

## Modes

MPLS RSVP mode (config-router-mpls-rsvp).

MPLS interface RSVP mode (config-router-mpls-eth-x/x-rsvp).

## Usage Guidelines

Summary refresh is a more effective tool for RSVP refresh message overhead reduction.

Use the **no** version of the command to disable RSVP bundle messages.

## Examples

The following commands enable RSVP bundle messages on interface *3/13* with a **bundle-send-delay** of *20* milliseconds.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 3/13
device(config-router-mpls-eth-3/13)# rsvp
device(config-router-mpls-eth-3/13-rsvp)# refresh-reduction bundle-message bundle-send-delay 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# region

Assigns a name to a Multiple Spanning Tree Protocol (MSTP) region.

## Syntax

**region** *region-name*

**no region**

## Parameters

*region-name*

Assigns a name to an MSTP region.

## Modes

Spanning tree MSTP configuration mode

## Usage Guidelines

The *region-name* string must be between 1 and 32 ASCII characters in length, and is case-sensitive.

Enter **no region** to delete the region name.

## Examples

To assign a name to an MSTP region named extreme1:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# region extreme1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# reliable-messaging

When RSVP reliable messaging is enabled on an interface of the SLX-OS device, RSVP trigger messages sent out on that interface includes a message ID and a request for acknowledgment from the RSVP neighbor.

## Syntax

```
reliable-messaging [ rapid-retrans-decay percent ] [ rapid-retrans-interval milliseconds ] [ rapid-retry-limit number ]
no reliable-messaging [ rapid-retrans-decay percent ] [ rapid-retrans-interval milliseconds ] [ rapid-retry-limit number ]
```

## Command Default

The command is disabled, by default.

## Parameters

### **rapid-retrans-decay** *percent*

Specifies the percentage increase in the rapid transmission interval for each consecutive unacknowledged RSVP message. The range is from 0 - 100, with a default of 100.

### **rapid-retrans-interval** *milliseconds*

Specifies the interval, in milliseconds, for an unacknowledged message to be resent. The range is from 100-30000 milliseconds, with a default of 2000 milliseconds.

### **rapid-retry-limit** *number*

Specifies the maximum number of retries for an unacknowledged message. The range is 1-16, with a default value of 5.

## Modes

MPLS interface RSVP mode (config-router-mpls-eth-x/x).

MPLS RSVP mode (config-router-mpls-rsvp).

## Usage Guidelines

When acknowledgment is not received, the trigger message is re-transmitted using the retransmission parameters configured on the interface.

The **no** form of the command removes reliable messaging.

## Examples

The following example enables RSVP reliable messaging on MPLS interface 3/13 .

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 3/13
device(config-router-mpls-eth-3/13)# rsvp
device(config-router-mpls-eth-3/13-rsvp)# reliable-messaging
```

The following example configures the **rapid-retrans-decay** option to *1* percent, the **rapid-retrans-interval** option to *100* milliseconds, and the **rapid-retry-limit** option to *1* try.

```
device# configure
device(config)# router-mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)# reliable-messaging rapid-retrans-decay 1 rapid-retrans-interval 100
rapid-retry-limit 1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# reload

Reboots the device, standby management module, or chassis.

## Syntax

```
reload { standby | system }
```

## Parameters

### standby

Reboots the standby management module.

### system

Reboots the chassis

## Modes

Privileged EXEC mode

## Usage Guidelines

All reboot operations are disruptive, and the commands prompt for confirmation before executing. When you reboot a device, all traffic to and from it stops. All ports on that device remain inactive until the device comes back online.

The **reload system** command performs a cold reboot that powers off and restarts the entire chassis. All session connections must be restarted. If the power-on self-test (POST) is enabled, POST is executed when the system comes back up.

### NOTE

Do not use the **reload** command without either the **standby** or **system** parameter.

## Examples

The following example performs a cold reboot of the device.

```
device# reload system
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rename

Renames a file in the device flash memory.

## Syntax

```
rename current_name new_name
```

## Parameters

*current\_name*

Specifies the file name you want to change.

*new\_name*

Specifies the new file name.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is supported only on the local device.

System configuration files cannot be renamed. If you try to rename a system file, a warning message is displayed.

## Examples

The following example renames a file in the flash memory.

```
device# rename myconfig myconfig_20101010
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# reoptimize-timer

The user can set a timer to optimize a specific LSP path on a periodic basis.

## Syntax

```
reoptimize-timer { seconds }
```

```
no reoptimize-timer { seconds }
```

## Command Default

The re-optimize timer is disabled, by default.

## Parameters

*seconds*

Specifies the length, in seconds, from the beginning of one re-optimization attempt to the beginning of the next attempt. The range is 300-65535 seconds.

## Modes

MPLS LSP configuration mode (`config-router-mpls-lsp-lsp_name`).

## Usage Guidelines

Until a commit is issued the re-optimize timer is disabled.

Configuring a re-optimization timer does not interfere with running the manual **reoptimize** command.

Time-triggered re-optimizing does not apply to LSPs within a FRR network.

When upgrading software, the configured adaptive LSPs are initialized with the no re-optimization timer.

## Examples

in the following example, the re-optimize time is configured to 1000 seconds, which specifies the number of seconds from the beginning of one re-optimization attempt to the beginning of the next attempt.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp to20
device(config-router-mpls-lsp-to20)# reoptimize-timer 1000
device(config-router-mpls-lsp-to20)# commit
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# resequence access-list

Reassigns sequence numbers to entries of an existing MAC, IPv4, or IPv6 access list.

## Syntax

```
resequence access-list { ip | ipv6 | mac } name seq_num increment
```

## Parameters

**ip | ipv6 | mac**

Specifies the Layer 2 or Layer 3 ACL bound to an interface.

*name*

Specifies the name of a standard or an extended ACL. A maximum of 63 characters is allowed.

*seq\_num*

Specifies the starting sequence number in the ACL. Valid values range from 1 through 65535.

*increment*

Specifies a value to increment the sequence number between rules. Valid values range from 1 through 65534.

## Modes

Privileged EXEC mode

## Usage Guidelines

Reordering the sequence numbers is useful when you need to insert rules into an existing ACL and there are not enough sequence numbers available. When all sequence numbers between rules are exhausted, this feature allows the reassigning of new sequence numbers to entries of an existing access list.

## Examples

The following example reorders the rules in a MAC ACL.

```
device# show running-config mac access-list test
!
mac access-list standard test
 seq 1 permit 0011.2222.3333
 seq 2 permit 0011.2222.4444
 seq 3 permit 0011.2222.5555
 seq 4 deny 0011.2222.6666
!
device# resequence access-list mac test 10 10

device# show running-config mac access-list test
!
mac access-list standard test
 seq 10 permit 0011.2222.3333
 seq 20 permit 0011.2222.4444
 seq 30 permit 0011.2222.5555
 seq 40 deny 0011.2222.6666
!
```

The following example reorders the rules in an IPv6 ACL.

```
device# show running-config ipv6 access-list distList
!
ipv6 access-list standard distList
 seq 10 deny 2001:125:132:35::/64
 seq 20 deny 2001:54:131::/64
 seq 30 deny 2001:5409:2004::/64
 seq 40 permit any!
device# resequence access-list ipv6 distList 100 100

device# show running-config ipv6 access-list distList
!
ipv6 access-list standard distList
 seq 100 deny 2001:125:132:35::/64
 seq 200 deny 2001:54:131::/64
 seq 300 deny 2001:5409:2004::/64
 seq 400 permit any
!
```

# reservable-bandwidth

The **reservable-bandwidth** command is configurable on an MPLS-enabled interface at any time. The configuration of the command takes effect immediately upon preemption of the LSP.

## Syntax

```
reservable-bandwidth { decimal | [ percentage decimal ] }
no reservable-bandwidth { decimal | [ percentage decimal ] }
```

## Command Default

The default value is the total physical bandwidth of the interface.

## Parameters

*decimal*

The decimal variable specifies a value from 0 through 2,000,000,000 in kbps.

**percentage***decimal*

The percentage decimal parameters specify a value from 0 through 100. The percentage value of 100 specifies that the entire interface bandwidth can be used by MPLS LSPs, when needed.

## Modes

MPLS interface mode (config-router-mpls-if-eth).

## Usage Guidelines

The no form of the command sets the maximum reservable bandwidth back to the default value.

When the maximum reservable bandwidth is configured as a percentage value for LAGs and VE interfaces, and ports go down, or new ports are added to the interface, the reservable bandwidth is recalculated as a percentage of the newly available bandwidth for that interface.

When the maximum reservable bandwidth is configured as either an absolute value, or a percentage value, the value is recalculated and updated to the latest value.

## Examples

The example below shows the configuration of the maximum reservable bandwidth for MPLS LSPs with an absolute value of 10000 kbps.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/1
device(config-router-mpls-if-eth-1/1)# reservable-bandwidth 10000
```

The following example configures the maximum reservable bandwidth as a percentage (80%) of the total interface bandwidth for the MPLS LSPs on the interface.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/1
device(config-router-mpls-if-eth-1/1)# reservable-bandwidth percentage 80
```

The following example shows when the maximum reservable bandwidth is changed from an absolute value to a percentage value, and vice versa, the following advisory message displays on the console to indicate the configuration change.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/1
device(config-router-mpls-if-eth-1/1)# reservable-bandwidth percentage 40
Maximum reservable bandwidth is changed from 30 kbps to 40%
```

The following example shows using the **no** form of the command to set the maximum reservable bandwidth back to the default value (the total physical bandwidth of the interface) when using the absolute value or percentage value.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/1
device(config-router-mpls-if-eth-1/1)# no reservable-bandwidth percentage 80
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# retransmit-interval

Sets the time the device waits before it retransmits Link State PDUs (LSPs).

## Syntax

```
retransmit-interval interval
```

```
retransmit-interval interval
```

## Command Default

The default retransmission interval is 5 seconds.

## Parameters

*secs*

Specifies the retransmission interval in seconds. Valid values range from 1 through 65535 seconds. The default is 5 seconds.

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command removes the configured interval.

## Examples

The following example changes the retransmission interval to 7 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# retransmit-interval 7
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## retry-limit

When the ingress LER fails to connect to the egress LER in a signaled LSP, the ingress LER tries indefinitely to make the connection unless the user sets a limit for these connection attempts. After this limit is exceeded, the ingress LER stops trying to connect to the egress LER over the primary path.

### Syntax

```
retry-limit { number }
no retry-limit
```

### Command Default

The command is disabled, by default.

### Parameters

*number*  
Specifies the LSP retry limit connection attempts.

### Modes

MPLS policy mode.

### Usage Guidelines

the no form of the command disables the configuration.

Once the connection is established, the retry counter is reset to zero.

### Examples

In the following example, when the LSP needs to be established again, the ingress LER makes 20 attempts to establish a connection to the egress LER.

```
device # configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# retry-limit 20
```

### History

Release version	Command history
16r.1.00	This command was introduced.

# retry-time

The user can configure the amount of time the ingress LER waits between connection attempts.

## Syntax

```
retry-time { seconds }
no retry-time
```

## Command Default

The command is disabled, by default.

## Parameters

*seconds*  
Specifies the LSP retry time in seconds. The default is 30 seconds.

## Modes

MPLS policy mode.

## Usage Guidelines

When a signaled LSP is enabled, the ingress LER attempts to connect to the egress LER over the primary path specified in the LSPs configuration. When the connection is not successful, by default the ingress LER waits 30 seconds before attempting the connection again.

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

## Examples

The following example configures the retry time to 45 seconds.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# retry-time 45
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# reverse-metric

Configures the reverse metric value at the Intermediate System-to-Intermediate System (IS-IS) router level.

## Syntax

```
reverse-metric [ value ] [ te-def-metric ] [ whole-lan ]
```

```
reverse-metric tlv-type [ value ]
```

```
no reverse-metric [ value ] [ te-def-metric ] [ whole-lan ]
```

```
no reverse-metric tlv-type [ value ]
```

## Command Default

The **reverse-metric** command is disabled by default.

## Parameters

<b>reverse-metric</b>	Specifies the reverse metric parameter at the IS-IS router level.
<b>value</b>	Specifies the reverse metric value in metric style. The metric style consists of narrow or wide style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default value is 16777214 irrespective of the metric style configured.
<b>te-def-metric</b>	Specifies that the device sends a traffic engineering (TE) default metric sub-type-length-value (TLV) within the reverse-metric TLV.
<b>whole-lan</b>	Specifies that the configured reverse metric value affects the entire LAN.
<b>tlv-type value</b>	Specifies the TLV type for the reverse metric value. The default value is 254.

## Modes

IS-IS router configuration mode

## Usage Guidelines

If the reverse-metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor device receives the reverse metric value through the IS hello, the neighbor router updates the cost to reach the original IS-IS router with the sum of default metric and the reverse metric value.

The **whole-lan** option only takes effect on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the **whole-lan** option is used.

The **no** form of the command specified with the configured value resets the metric value to the default value of 16777214. The **no reverse-metric** command removes the entire reverse metric configuration.



## Examples

The following example changes the reverse metric value for the entire LAN to 50.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# reverse-metric 50 whole-lan
```

The following example configures the reverse metric TLV type in the range of unassigned IS-IS TLV values.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# reverse-metric tlv-type 230
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## revert-timer

The path selection revert timer provides an option to stabilize a path before traffic is switched to it. Without a configured path selection revert timer, the router switches between a primary and secondary path immediately after the current working path goes down.

### Syntax

```
revert-timer { timer_value }  
no revert-timer
```

### Command Default

There is no revert-timer in the default command mode.

### Parameters

*timer\_value*

The number of seconds that the router waits after the primary or selected path comes up before traffic reverts to that path. The range is 1- 65,535 seconds.

### Modes

MPLS LSP configuration mode (*config-router-mpls-lsp-lsp\_name*).

### Usage Guidelines

The **revert-timer** command has no effect on the unconditional select mode. Traffic is unconditionally switched to the user selected path and stays on it.

The path stability test used with the revert timer is based on the uptime of the latest instance of the path. This value can be different when the selected path has gone through a "make-before-break" procedure.

For an LSP going through re-optimization, the new LSP does not carry traffic until the revert timer expires.

When a user changes the revert timer, the basis of counting is the uptime of the path and is independent of the sequence or combination of configurations.

The **no** form of the command removes the revert-timer.

### Examples

The following example configures the revert-timer to 10 seconds.

```
device# configure  
device(config)# router mpls  
device(config-router-mpls)# lsp samplelsp  
device(config-router-mpls-lsp-samplelsp)# revert-timer 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# revertive global

The revertive mode global command can be executed only on LSPs with FRR and adaptive enabled.

## Syntax

```
revertive global [ disable | enable ]  
no revertive mode global
```

## Command Default

Global revertiveness is enabled by default for LSPs with FRR and adaptive enabled.

## Parameters

**disable**  
Disables global revertiveness.

**enable**  
Enables global revertiveness.

## Modes

MPLS LSP Fast Reroute.

## Usage Guidelines

The **no** option disables global revertiveness on an LSP.

When adaptive is disabled, then global revertiveness is also disabled.

## Examples

The following example enables global revertiveness on LSP *t1*.

```
device# config  
device(config)# router mpls  
device(config-router-mpls)# lsp t1  
device(config-router-mpls-lsp-t1)# adaptive  
device(config-router-mpls-lsp-t1)# frr  
device(config-router-mpls-lsp-t1-frr)# revertive global enable
```

The following example is of an adaptive LSP.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# to 10.3.3.3
device(config-router-mpls-lsp-t1)# from 10.2.2.2
device(config-router-mpls-lsp-t1)# traffic-eng mean-rate 1000
device(config-router-mpls-lsp-t1)# adaptive
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# facility-backup
device(config-router-mpls-lsp-t1-frr)# exit
device(config-router-mpls-lsp-t1)# enable
device(config-router-mpls)#
```

The following example changes the FRR bandwidth for an adaptive LSP.

```
device(config)#
device(config)# router mpls
device(config-router-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# bandwidth 1000
device(config-router-mpls-lsp-t1-frr)# exit
device(config-router-mpls-lsp-t1)# commit
```

The following example show how global revertiveness is enabled by default in FRR mode for an adaptive LSP.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# retry-limit 20
device(config-router-mpls-policy)# exit
device(config-router-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# adaptive
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# revertive mode global
device(config-router-mpls-lsp-t1-frr)# revertive holdtime 20
device(config-router-mpls-lsp-t1-frr)# exit
device(config-router-mpls-lsp-t1)# commit
device(config-router-mpls-lsp-t1)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# revertive hold-time

Specifies the time, in seconds, the LSP holds before attempting a new path on the FRR LSP.

## Syntax

```
revertive holdtime { value }
no revertive holdtime
```

## Command Default

The default is five seconds.

## Parameters

*value*

Specifies the hold time value in seconds. The hold-time is the time between the primary LSP failure and the trigger of new instance of LSP by global reversioness. The range is one through 60 seconds.

## Modes

MPLS LSP fast reroute mode (config-router-mpls-lsp-lsp\_name-frr).

## Usage Guidelines

The **no** form of the command removes the revertive hold time.

## Examples

The following example configures the revertive hold time to 20 seconds.

```
device# configure
device(Config)# router mpls
device(config-router-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# adaptive
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# revertive mode global
device(config-router-mpls-lsp-t1-frr)# revertive holdtime 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# revision

Assigns a version number to the Multiple Spanning Tree Protocol (MSTP) configuration.

## Syntax

**revision** *number*  
**no revision**

## Command Default

The default is 0.

## Parameters

*number*  
 Specifies the revision or version number of the MSTP region. Valid values range from 0 through 255.

## Modes

]Spanning tree MSTP configuration mode

## Usage Guidelines

Enter **no revision** to return to the default setting.

## Examples

To set the configuration revision to 1:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# revision 1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rfc1583-compatibility (OSPF)

Configures compatibility with RFC 1583.

## Syntax

```
rfc1583-compatibility
no rfc1583-compatibility
```

## Command Default

OSPF is compatible with RFC 1583 (OSPFv2).

## Modes

OSPF router configuration mode  
OSPF router VRF configuration mode

## Usage Guidelines

OSPF is compatible with RFC 1583 (OSPFv2) and maintains a single best route to an autonomous system (AS) boundary router in the OSPF routing table. Disabling this compatibility causes the OSPF routing table to maintain multiple intra-AS paths, which helps prevent routing loops.

Enter **no rfc1583-compatibility** to disable compatibility with RFC 1583.

## Examples

The following example disables compatibility with RFC 1583.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# no rfc1583-compatibility
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# rib-route-limit

Limits the maximum number of BGP Routing Information Base (RIB) routes that can be installed in the Routing Table Manager (RTM).

## Syntax

```
rib-route-limit num
```

```
no rib-route-limit
```

## Command Default

This option is disabled. There is no limit.

## Parameters

*num*

Decimal value for the maximum number of RIB routes to be installed in the RTM. Range is from 1 through 4294967295.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

This command controls the number of routes installed by BGP, irrespective of whether those BGP routes are the preferred routes in the system. BGP locally tracks the number of routes installed and the number of routes withdrawn from RIB. If the total number of routes installed exceeds the value specified by *num*, routes will not be installed.

If *num* is increased, route calculation is automatically triggered.

If *num* is decreased, the user is prompted to clear the BGP RTM.

## Examples

This example configures the device to limit the maximum number of BGP4 RIB routes that can be installed in the RTM.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# rib-route-limit 10000
```

This example configures the device to limit the maximum number of BGP4+ RIB routes that can be installed in the RTM in VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# rib-route-limit 32000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rmon alarm

Sets the RMON alarm conditions.

## Syntax

```
rmon alarm index snmp_oid interval seconds [ absolute | delta ] rising-threshold value event number [ falling-threshold value event number [ owner name ]
```

```
no rmon alarm
```

## Command Default

No alarms are configured.

## Parameters

*index*

Specifies the RMON alarm index. Valid values range from 1 through 65535.

*snmp\_oid*

Specifies the MIB object to monitor. The variable must be in the SNMP OID format, for example, 1.3.6.1.2.1.16.1.1.1.5.65535. The object type must be a counter32.

**interval** *seconds*

Specifies the RMON alarm sample interval in seconds. Valid values range from 1 through 2147483648.

**absolute**

Sets the sample type as absolute.

**delta**

Sets the sample type as delta.

**rising-threshold** *value*

Specifies the RMON alarm rising threshold. Valid values range from 0 through 4294967295.

**event** *number*

Specifies the event for the rising alarm. Valid values range from 1 through 65535.

**falling-threshold** *value*

Specifies the RMON alarm falling threshold. Valid values range from 0 through 4294967295.

**event** *number*

Specifies the event for the rising alarm. Valid values range from 1 through 65535.

**owner** *name*

Specifies the identity of the owner. The maximum number of characters is 32.

## Modes

Global configuration mode

## Usage Guidelines

Enter **no rmon alarm** to disable the alarm conditions.

## Examples

To set RMON alarm conditions:

```
device# configure terminal
device(config)# rmon alarm 100 1.3.6.1.2.1.16.1.1.1.5.65535 interval 5 absolute rising-threshold 10000
event 100 falling-threshold 1000 event 101 owner admin
```

# rmon collection history

Collects Ethernet group statistics for later retrieval.

## Syntax

```
rmon collection history number [ buckets bucket_number | interval seconds | owner name ]
```

```
no rmon collection history number
```

## Command Default

RMON history collection is not enabled.

## Parameters

*number*

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

**buckets** *bucket\_number*

Specifies the maximum number of buckets for the RMON collection history. Valid values range from 1 through 65535.

**interval** *seconds*

Specifies the alarm sample interval in seconds. Valid values range from 1 through 3600. The default value is 1800.

**owner** *name*

Specifies the identity of the owner. The maximum number of characters is 15.

## Modes

Interface subtype configuration mode

## Usage Guidelines

This command collects periodic statistical samples of Ethernet group statistics on a specific interface for later retrieval.

Enter **no rmon collection history** *number* to disable the history of statistics collection.

## Examples

To collect RMON statistics, with an RMON collection control index value of 5 for the owner named admin, on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# rmon collection history 5 owner admin
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rmon collection stats

Collects Ethernet group statistics on a specific interface.

## Syntax

**rmon collection stats** *number* [ **owner name** ]

**no rmon collection stats** *number*

## Command Default

RMON statistic collection is not enabled.

## Parameters

*number*

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

**owner name**

Specifies the identity of the owner.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Enter **no rmon collection stats** *number* to disable the collection of statistics.

Ethernet group statistics collection is not supported on ISL links.

## Examples

The following example shows how to collect RMON statistics, with an RMON collection control index value of 2 for the owner named admin, on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# rmon collection stats 2 owner admin
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rmon event

Adds or removes an event in the RMON event table associated to the RMON alarm number.

## Syntax

```
rmon event index [ description word | log | owner name | trap word ]  
no rmon event
```

## Command Default

No events are configured.

## Parameters

*index*

Specifies the RMON event number. Valid values range from 1 through 65535.

*description word*

Specifies a description of the event.

log

Generates an RMON log when an event is triggered.

*owner name*

Specifies the owner of the event. The *name* string must be between 1 and 32 characters in length.

*trap word*

Specifies the SNMP community or string name to identify this trap.

## Modes

Global configuration mode

## Usage Guidelines

Enter **no rmon event** to remove the event configuration.

## Examples

To configure an RMON event:

```
device# configure terminal  
device(config)# rmon event 2 log description "My Errorstoday" owner gjack
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# role name

Creates or modifies a non-default role.

## Syntax

**role name** *role\_name* [ **desc** *description* ]

**no role name** *role\_name* [ **desc** *description* ]

## Parameters

*role\_name*

Specifies the name of the role.

**desc** *description*

Specifies an optional role description.

## Modes

Global configuration mode

## Usage Guidelines

For each role that you create, you define one or more rules. Each user is associated with one—and only one—role.

Role names are from 4 through 32 characters, must begin with a letter, and can contain alphanumeric characters and underscores. The name cannot be same as that of an existing user.

The description field supports up to 64 characters and can include any printable ASCII character, except for the following characters: single quotation mark ('), double quotation mark ("), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces, enclose the text in double quotation marks.

The maximum number of roles supported is 64, including the user and admin default roles.

To delete a role description, enter **no role name** *role\_name* **desc**.

To delete a role, enter **no role name** *role\_name*.

## Examples

The following example creates a role.

```
device# configure terminal
device(config)# role name tempAdmin desc "Daily admin functions"
```

The following example deletes the role.

```
device# configure terminal
device(config)# no role name tempAdmin
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# router bgp

Enables BGP routing.

## Syntax

`router bgp`

## Command Default

BGP routing is not enabled.

## Modes

Global configuration mode

## Usage Guidelines

The **no** form of the command disables BGP routing.

## Examples

This example enables BGP routing.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing.

## Syntax

```
router isis
```

## Command Default

Disabled

## Modes

Global configuration mode

## Usage Guidelines

The **no** form of the command disables IS-IS routing.

## Examples

The following example enables IS-IS routing.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# router mpls

Enables MPLS and accesses MPLS configuration mode

## Syntax

`router mpls`

`no router mpls`

## Command Default

MPLS is disabled by default.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no** form of this command to disable MPLS on the device.

## Examples

The following example enables MPLS on the device and access MPLS configuration mode.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# router ospf

Enables and configures the Open Shortest Path First version 2 (OSPFv2) routing protocol.

## Syntax

```
router ospf [ vrf name ]
no router ospf
```

## Command Default

Disabled.

## Parameters

**vrf name**  
Specifies a nondefault VRF.

## Modes

Global configuration mode

## Usage Guidelines

Use this command to enable the OSPFv2 routing protocol and enter OSPF router or OSPF router VRF configuration mode. OSPFv2 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

The **no** form of the command deletes all current OSPF configuration and blocks any further OSPFv2 configuration.

## Examples

The following example enables OSPFv2 on a default VRF and enters OSPF VRF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# router pim

Configures basic global protocol-independent multicast (PIM) Sparse parameters on a device within the PIM Sparse domain and enters PIM-router configuration mode.

## Syntax

```
router pim
```

```
no router pim
```

## Command Default

PIM Sparse is not configured.

## Modes

Global configuration mode

## Usage Guidelines

The **no** form of this command disables PIM and removes all configuration for PIM multicast on the device (**router pim** level) only.

You do not need to globally enable IP multicast routing when configuring PIM Sparse.

After you enable IP multicast routing and PIM Sparse at the global level, you must enable it on the individual interfaces connected to the PIM Sparse network.

If you configure PIM Sparse on an interface that is on the border of the PIM Sparse domain, you also must also configure the **ip pim border** command on the interface.

You must configure the **bsr-candidate ethernet** command to identify an interface on at least one device as a candidate PIM Sparse Bootstrap router (BSR) and candidate PIM Sparse Rendezvous Point (RP).

You can configure the **rp-address** command to explicitly identify an RP, including an ACL-based RP, by its IP address instead of having it identified by the RP election process.

## Examples

This example configures basic global PIM Sparse parameters.

```
device(config)# router pim
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# route-precedence

Configures a table that defines the order (precedence) in which multicast routes are selected from the multicast routing table (mRTM) and unicast routing (uRTM) table.

## Syntax

```
route-precedence { [ none | uc-default |uc-non-default ] | [ uc-default | none |uc-non-default ] | [ uc-non-default | none |uc-
default ] }
```

```
no route-precedence
```

## Command Default

The default route precedence used to select routes is **uc-non-default** followed by **uc-default**.

## Parameters

### none

Specifies that this type of route is to be ignored. You can specify this option for any of the multicast or unicast route types.

### uc-non-default

Specifies the precedence for the non-default unicast route table (uRTM).

### uc-default

Specifies the precedence for the default unicast route table (uRTM).

## Modes

Router PIM configuration mode

## Usage Guidelines

The order in which you place the keywords determines the route precedence.

The **no** form of this command restores the default route precedence settings.

## Examples

The following example configures the route precedence.

```
device(config)# router pim
device(config-pim-router)# route-precedence uc-default uc-non-default none
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rp-address

Configures a device interface as a rendezvous point (RP).

## Syntax

```
rp-address ip-address
```

```
no rp-address ip-address
```

## Command Default

The RP is selected by the PIM Sparse protocol's RP election process.

## Parameters

*ip-address*

Specifies the IPv4 address of the RP.

## Modes

Router PIM configuration mode

## Usage Guidelines

The **no** form of this command restores the default and the RP is selected by the RP election process.

Devices in the PIM Sparse domain use the specified RP and ignore group-to-RP mappings received from the bootstrap router (BSR).

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the BSR sends to each of the PIM Sparse routers.

## Examples

This example configures the device interface at IP address 4.4.4.4 as the RP for the PIM Sparse domain. The default group range is 224/4.

```
device(config)# router pim
device(config-pim-router)# rp-address 4.4.4.4
```

This example configures the RP with specific group ranges:

```
device(config)# router pim
device(config-pim-router)# rp-address 4.4.4.4 static-rp-plist
device(config)# ip prefix-list static-rp-plist permit 225.1.1.0/24
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rp-candidate

Configures a device as a candidate rendezvous point (RP) for all multicast groups with the prefix 224.0.0.0/4, by default, and explicitly adds or deletes groups with other prefixes.

## Syntax

```
rp-candidate [ interface interface type | prefix IP prefix-list name ]
```

## Command Default

The PIM router is not available for selection as an RP.

## Parameters

**interface** *interface type*

Specifies an interface for the candidate RP. Interface types include ethernet, loopback, port-channel, and Ve.

**prefix** *IP prefix list name*

Specifies the IP prefix list name.

## Modes

Router PIM configuration mode

## Usage Guidelines

The **no rp-candidate** command makes the PIM router cease to act as a candidate RP.

Configuring the **rp-candidate** command on an Ethernet, loopback, virtual, or tunnel interface, configures the device as a candidate RP for all multicast groups with the prefix 224.0.0.0/4, by default. You can configure the **rp-candidate add** command to add to those a group address or range of group addresses. You can configure the **rp-candidate delete** command to delete a group address or range of group addresses that were added to the default addresses.

### NOTE

You cannot delete the default group prefix.

The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the bootstrap router (BSR) sends to each of the PIM Sparse routers.

Although you can configure the device as only a candidate BSR or an RP, it is recommended that you configure the same interface on the same device as both a BSR and an RP.

## Examples

This example configures a physical device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate ethernet 1/1
```

This example configures a loopback interface as a candidate RP:

```
device(config-pim-router)# rp-candidate interface loopback 11
device(config-pim-router)# rp-candidate prefix my-rp-cand-list
device(config)# ip prefix-list my-rp-cand-list permit 226.1.1.0/24
device(config)# ip prefix-list my-rp-cand-list permit 228.1.1.0/24
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rpf ecmp rebalance

Enables multicast ECMP load sharing with dynamic rebalancing.

## Syntax

**rpf ecmp rebalance**

**no rpf ecmp rebalance**

## Modes

Router PIM configuration mode

## Usage Guidelines

Once you configure ECMP rebalance the existing flows are redistributed among the all available ECMP paths. In addition, whenever a new next-hop is added, some of the existing flows are redistributed to the new path added using the newly added ECMP path.

## Examples

The following example enables multicast ECMP load sharing with dynamic rebalancing.

```
device(config)# router pim
devic(config-pim-router)# rpf ecmp rebalance
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## rsvp

Accesses MPLS RSVP configuration mode to configure RSVP-TE Hello.

## Syntax

```
rsvp
no rsvp
```

## Command Default

None

## Modes

MPLS configuration mode  
MPLS interface configuration mode

## Examples

The following example accesses MPLS RSVP configuration mode to configure RSVP-TE Hello globally.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)#
```

The following example accesses MPLS RSVP configuration mode to configure RSVP-TE Hello on an MPLS interface.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/12
device(config-router-mpls-interface-1/12)# rsvp
device(config-router-mpls-interface-1/12-rsvp)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rsvp-flooding-threshold

The **rsvp-flooding-threshold** command can be executed multiple times for the same interface. The threshold values are added to the existing set of values for the interface.

## Syntax

```
rsvp-flooding-threshold [ down | up ] percent *
no rsvp-flooding-threshold [ down | up ] percent *
```

## Command Default

The command is disabled, by default.

## Parameters

### down percent\*

The down option sets the thresholds for decreased resource availability. Valid values are from 0 to 99. The default values for down is 100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, 15.

The "\*" represents multiple percent values can be given. A minimum one percentage value is required.

### up percent\*

The up option sets the thresholds for increased resource availability. Valid values are from 1 to 100. The default values for up is 15, 30, 45, 60, 75, 80, 85, 90, 95, 97, 98, 99, 100.

The "\*" represents multiple percent values can be given. A minimum one percentage value is required.

## Modes

MPLS policy mode.

## Usage Guidelines

The **no** form of the command removes the RSVP TE flooding threshold configuration.

Previously configured values are not overwritten. The interface specific configuration overrides the global configuration.

## Examples

In the following example, the UP thresholds contain 10, 50, 55, 95, 96, 97, 98, and 100. The DOWN thresholds contain 50, 40, 30, 20, and 10.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/1
device(config-router-mpls-if-eth-1/1)# rsvp-flooding-threshold up 10 50 55 95
device(config-router-mpls-if-eth-1/1)# rsvp-flooding-threshold up 96 97 98 99 100
device(config-router-mpls-if-eth-1/1)# rsvp-flooding-threshold down 50 40
device(config-router-mpls-if-eth-1/1)# rsvp-flooding-threshold down 30 20 10
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# rsvp-periodic-flooding-time

Sets the interval for RSVP-TE periodic flooding.

## Syntax

```
rsvp-periodic-flooding-time { interval }
no rsvp-periodic-flooding-time
```

## Command Default

All MPLS interfaces are checked every three minutes by default. The length of interval value is set to zero.

## Parameters

*interval*

Specifies the length of interval used for periodic flooding (in seconds). Valid range is zero, 30–3600. For value zero, periodic flooding is turned off.

## Modes

MPLS policy mode.

## Usage Guidelines

TE advertisements are triggered when there is a difference in the available bandwidth and advertised available bandwidth.

The **no** form of the command can be used to set the periodic flooding timer to default value.

## Examples

The following example sets the interval as 240, which triggers periodic flooding every four minutes.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# rsvp-periodic-flooding-time 240
device(config-router-mpls-policy)# no rsvp-periodic-flooding-time
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rule

Creates role-based access permissions (RBAC) associated with a role.

## Syntax

```
rule index [ action { accept | reject } ] [ operation { read-only | read-write } ] role role_name command command_name
no rule index
```

## Command Default

The default for **action** is **accept**. The default for **operation** is **read-write**.

## Parameters

*index*

Specifies a numeric identifier for the rule. Valid values range from 1 through 512.

**action** **accept** | **reject**

(Optional) Specifies whether the user is accepted or rejected while attempting to execute the specified command. The default value is **accept**.

**operation** **read-only** | **read-write**

(Optional) Specifies the type of operation permitted. The default value is **read-write**.

**role** *role\_name*

Specifies the name of the role for which the rule is defined.

**command** *command\_name*

Specifies the command for which access is defined. Separate commands with a space. To display a list of supported commands, type a question mark (?).

## Modes

Global configuration mode

## Usage Guidelines

For each role that you create, you define one or more rules. Each account is associated with one—and only one—role.

When you create a rule, the *index*, **role**, and **command** operands are mandatory; the **action** and **operation** operands are optional.

The maximum number of rules is 512.

When you modify a rule, all operands except *index* and **role** are optional.

Enter **no rule** *index* to remove the specified rule.

## Examples

The following example creates rules enabling the NetworkSecurityAdmin role to create user accounts.

```
device# configure terminal
device(config)# rule 150 action accept operation read-write role NetworkSecurityAdmin command config
device(config)# rule 155 action accept operation read-write role NetworkSecurityAdmin command username
```

The following example deletes a rule.

```
device# configure terminal
device(config)# no rule 155
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# rx-label-silence-time

Defines the length of the receive label silence timer for for LDP-IGP synchronization.

## Syntax

`rx-label-silence-time` *milliseconds*

`no rx-label-silence-time`

## Command Default

The default value is 1000 milliseconds.

## Parameters

*milliseconds*

Specifies the length of time in milliseconds of the receive label silence timer. Enter an integer from 100 to 60000.

## Modes

MPLS LDP configuration mode

## Usage Guidelines

Use the **no** form of the command to reset the default value of 1000 milliseconds.

When labels are not received from the peer for a short period of time, the session is declared In Sync. When a label is received from a peer, then the receive label silence timer is reset.

## Examples

The following example sets the length of time for the receive label silence timer to 80000 milliseconds.

```
device(conf)# router mpls
device(config-mpls)# ldp
device(config-router-mpls-ldp)# rx-label-silence-time 80000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# sample-recording

Configures the template to record the sample history.

## Syntax

```
sample-recording [ disable | enable ]
```

```
no sample-recording
```

## Command Default

The command is disabled by default.

## Parameters

### disable

Removes the setting for the sample recording for the selected LSP or autobw-template.

### enable

Sets the sample recording for ththe selected LSP or autobw-template.

## Modes

MPLS sub-configuration modes.

```
config-router-mpls-autobw-template-template1
```

```
config-router-mpls-lsp-lsp1
```

## Usage Guidelines

The **no** function of the command disables the option..

## Examples

## History

Release version	Command history
16r.1.00	This command was introduced.

# seq (rules in IPv4 extended ACLs)

Inserts filtering rules in IPv4 extended ACLs. Extended ACLs permit or deny traffic according to source and destination addresses, as well as other parameters.

## Syntax

```
[ seq seq-value ] permit ip-protocol { S_IPAddress [ mask ] | host S_IPAddress | any } [ source-operator [ S_port-numbers ] ]
  { D_IPAddress [ mask ] | host D_IPAddress | any } [ dscp DSCPvalue | dscp-force ] [ destination-operator [ D_port-
  numbers ] ] [ vlan vlanID ] [ TCP-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]

[ seq seq-value ] { deny | hard-drop } ip-protocol { S_IPAddress [ mask ] | host S_IPAddress | any } [ source-operator [ S_port-
  numbers ] ] { D_IPAddress [ mask ] | host D_IPAddress | any } [ dscp DSCPvalue ] [ destination-operator [ D_port-
  numbers ] ] [ vlan vlanID ] [ TCP-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]

no seq seq-value

no permit ip-protocol { S_IPAddress [ mask ] | host S_IPAddress | any } [ source-operator [ S_port-numbers ] ] { D_IPAddress
  [ mask ] | host D_IPAddress | any } [ dscp DSCPvalue | dscp-force ] [ destination-operator [ D_port-numbers ] ] [ vlan
  vlanID ] [ TCP-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]

no { deny | hard-drop } ip-protocol { S_IPAddress [ mask ] | host S_IPAddress | any } [ source-operator [ S_port-numbers ] ]
  { D_IPAddress [ mask ] | host D_IPAddress | any } [ dscp DSCPvalue ] [ destination-operator [ D_port-numbers ] ] [ vlan
  vlanID ] [ TCP-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]
```

## Parameters

### seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq seq-value**, the rule is added at the end of the list.

*seq-value*

Valid values range from 1 through 65535.

### permit

Specifies rules to permit traffic.

### deny

Specifies rules to deny traffic.

### hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

### ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:

<0-255>

Protocol number custom value from 0 through 255.

icmp

Internet Control Message Protocol

ip

Any IP protocol

**tcp**  
(Supported only if the containing ACL is applied to incoming traffic) Transmission Control Protocol

**udp**  
User Datagram Protocol

*S\_IPAddress*  
Specifies a source address for which you want to filter the subnet.

*mask*  
Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

**host**  
Specifies a source address.

*S\_IPAddress*  
The source address.

**any**  
Specifies all source addresses.

*source-operator* and *destination-operator*  
If you specified **tcp** or **udp** *ip-protocol*, the following optional operators are available:

**eq**  
The policy applies to the TCP or UDP port name or number you enter after **eq**.

**gt**  
The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt**.

**lt**  
The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt**.

**neq**  
The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

**range**  
The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: **range 23 53** (two values separated by a space). The first port number in the range must be lower than the last number in the range.

*S\_port-numbers* and *D\_port-numbers*  
(Valid only when *ip-protocol* is UDP or TCP) Specifies one or more source or destination port numbers.

*D\_IPAddress*  
Specifies a destination address for which you want to filter the sub-net.

*mask*  
Defines a mask, whose effect is to specify a subnet that includes the destination address that you specified. For options to specify the mask, see the Usage Guidelines.

**host**  
Specifies a destination address.



*D\_IPAddress*

The destination address.

**any**

Specifies all destination addresses.

**dscp**

Matches *DSCPvalue* against the DSCP value of the packet.

*DSCPvalue*

From 0 through 63.

**dscp-force**

(In **permit** rules, for incoming routed packets) Forces the outgoing DSCP value of packets that match the filter.

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

(Currently not supported) (In **permit** rules for incoming traffic) Sets the force drop precedence by the specified value.

**vlan** *vlanID*

Specifies a VLAN interface to which the ACL is bound.

*TCP-flags*

If you specify **tcp ip-protocol**, one or more of the following flags are available:

**ack**

Filters packets for which the **ack** (acknowledge) flag is set.

**fin**

Filters packets for which the **fin** (finish) flag is set.

**rst**

Filters packets for which the **rst** (reset) flag is set.

**sync**

Filters packets for which the **syn** (synchronize) flag is set.

**urg**

Filters packets for which the **urg** (urgent) flag is set.

**push**

Filters packets for which the **psh** (push) flag is set.

**count**

Enables statistics for the rule.

**log**

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

**mirror**

(Supported for rules in ACLs applied on physical interfaces to inbound traffic. Not supported for PBR, rACLs, or ACL-RL.) Mirrors packets matching the rule.

**copy-sflow**

Sends matching inbound packets to the sFlow collector.

## Modes

ACL configuration mode

## Usage Guidelines

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The **hard-drop** keyword is equivalent to the **deny** keyword.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

Although in an extended-ACL rule you can specify **mirror**, **log**, and **copy-sflow**, only one of the three is processed, as follows:

- In a permit rule, the order of precedence is **mirror > copy-sflow > log**.
- In a deny or hard-drop rule, the order of precedence is **log > copy-sflow > mirror**.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not applied.

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL, from an interface-subtype configuration mode you use the { **ip | ipv6 | mac** } **access-group** command.
- To apply a receive-path ACL, from global configuration mode, you use the { **ip | ipv6** } **receive access-group** command.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq seq-value**.
- If you do not know the rule number, type **no** followed by the full syntax without **seq seq-value**.

## Examples

The following example creates an IPv4 extended ACL and defines rules.

```
device(config)# ip access-list extended extdACL5
device(config-ipacl-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
device(config-ipacl-ext)# seq 7 deny tcp any any eq 80
device(config-ipacl-ext)# seq 10 deny udp any any range 10 25
device(config-ipacl-ext)# seq 15 permit tcp any any
```

The following example creates an IPv4 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ip access-list extended ipv4-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20.0.0.1 count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq bgp count
device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.3 host 224.0.0.1 count
device(conf-ipacl-ext)# exit
device(config)# ip receive access-group ipv4-receive-acl-example
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# seq (rules in IPv4 standard ACLs)

Inserts filtering rules in IPv4 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

## Syntax

```
seq seq-value { permit | deny | hard-drop } { S_IPAddress [ mask ] | host S_IPAddress | any } [ count ] [ log ] [ copy-sflow ]
{ permit | deny | hard-drop } { S_IPAddress [ mask ] | host S_IPAddress | any } [ count ] [ log ] [ copy-sflow ]
no seq seq-value
no { permit | deny | hard-drop } { S_IPAddress [ mask ] | host S_IPAddress | any } [ count ] [ log ] [ copy-sflow ]
```

## Parameters

### seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq seq-value**, the rule is added at the end of the list.

*seq-value*

Valid values range from 1 through 65535.

### permit

Specifies rules to permit traffic.

### deny

Specifies rules to deny traffic.

### hard-drop

Specifies rules to deny traffic.

### *S\_IPAddress*

Specifies a source address for which you want to filter the subnet.

*mask*

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

### host

Specifies a source address.

*S\_IPAddress*

The source address.

### any

Specifies all source addresses.

### count

Enables statistics for the rule.

### log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

### copy-sflow

(For incoming traffic) Sends matching packets to the sFlow collector.

## Modes

ACL configuration mode

## Usage Guidelines

This command configures rules to permit or drop traffic based on source addresses. You can also enable counters, logging, and sFlow.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The **hard-drop** keyword is equivalent to the **deny** keyword.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

Although in a standard-ACL rule you can specify both **log** and **copy-sflow**, only one of the two is processed, as follows:

- In a permit rule, only **copy-sflow** is processed.
- In a deny or hard-drop rule, only **log** is processed.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not applied.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq seq-value**.
- If you do not know the rule number, type **no** and then enter the full syntax without **seq seq-value**.

## Examples

The following example shows how to create a IPv4 standard ACL, define rules for it, and apply the ACL to an interface:

```
device# configure
device(config)# ip access-list standard stdACL3
device(config-ipacl-std)# seq 5 permit host 10.20.33.4
device(config-ipacl-std)# seq 15 deny any
device(config-ipacl-std)# exit
device(config)# interface ethernet 2/5
device(conf-if-eth-2/5)# ipv4 access-group stdACL3 in
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# seq (rules in IPv6 extended ACLs)

Inserts filtering rules in IPv6 extended ACLs. IPv6 extended ACLs permit or deny traffic according to source address, as well as other parameters.

## Syntax

```
[ seq seq-value ] permit ip-protocol { any | S_IPAddress / prefix_len | host S_IPAddress } [ source-operator [ S_port-numbers ] ] { any | D_IPAddress / prefix_len | host D_IPAddress } [ destination-operator [ D_port-numbers ] ] [ dscp DSCPvalue | dscp-force ] [ vlan vlanID ] [ tcp/udp-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]

[ seq seq-value ] { deny | hard-drop } ip-protocol { any | S_IPAddress / prefix_len | host S_IPAddress } [ source-operator [ S_port-numbers ] ] { any | D_IPAddress / prefix_len | host D_IPAddress } [ destination-operator [ D_port-numbers ] ] [ dscp DSCPvalue ] [ vlan vlanID ] [ tcp/udp-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]

no seq seq-value

no permit ip-protocol { any | S_IPAddress / prefix_len | host S_IPAddress } [ source-operator [ S_port-numbers ] ] { any | D_IPAddress / prefix_len | host D_IPAddress } [ destination-operator [ D_port-numbers ] ] [ dscp DSCPvalue | dscp-force ] [ vlan vlanID ] [ tcp/udp-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]

no { deny | hard-drop } ip-protocol { any | S_IPAddress / prefix_len | host S_IPAddress } [ source-operator [ S_port-numbers ] ] { any | D_IPAddress / prefix_len | host D_IPAddress } [ destination-operator [ D_port-numbers ] ] [ dscp DSCPvalue ] [ vlan vlanID ] [ tcp/udp-flags ] [ count ] [ log ] [ mirror ] [ copy-sflow ]
```

## Parameters

### seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq seq-value**, the rule is added at the end of the list.

*seq-value*

Valid values range from 1 through 65535.

### permit

Specifies rules to permit traffic.

### deny

Specifies rules to deny traffic.

### hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

### ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:

<0-255>

Protocol number custom value from 0 through 255.

### ipv6-icmp

Internet Control Message Protocol

### ipv6

Any IP protocol

**tcp**  
Transmission Control Protocol

**udp**  
User Datagram Protocol

**any**  
Specifies all source addresses.

*S\_IPAddress*  
Specifies a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

*prefix\_len*  
Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

**host**  
Specifies a source address.

*S\_IPAddress*  
The specific address. For options to abbreviate the address, see the Usage Guidelines.

*source-operator*  
If you specified **tcp** or **udp ip-protocol**, the following optional operators are available:

**eq**  
The policy applies to the TCP or UDP port name or number you enter after **eq**.

**gt**  
The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt**.

**lt**  
The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt**.

**neq**  
The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

**range**  
The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: **range 23 53** (two values separated by a space). The first port number in the range must be lower than the last number in the range.

*S\_port-numbers*  
(Valid only when *ip-protocol* is UDP or TCP) Specify one or more port numbers.

**any**  
Specifies all destination addresses.

*D\_IPAddress*  
Specifies a destination address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

*prefix\_len*  
Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

**host**

Specifies a destination address.

*D\_IPAddress*

The destination address. For options to abbreviate the address, see the Usage Guidelines.

*destination-operator*

Specifies one of the following destination operators:

**eq**

The policy applies to the TCP or UDP port name or number you enter after **eq**.

**gt**

The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt**.

**lt**

The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt**.

**neq**

The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.

**range**

The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53. The first port number in the range must be lower than the last number in the range.

*D\_port\_numbers*

(Valid only when *ip-protocol* is UDP or TCP) Specify one or more destination port numbers.

**dscp**

Matches *DSCPvalue* against the DSCP value of the packet.

*DSCPvalue*

From 0 through 63.

**dscp-force**

(In **permit** rules, for routed packets) Forces the outgoing DSCP value of packets that match the filter.

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

(Currently not supported) (In **permit** rules) Sets the force drop precedence by the specified value.

**vlan** *vlanID*

Specifies a VLAN interface to which the ACL is bound.

*tcp/udp-flags*

If you specify **tcp** or **udp** *ip-protocol*, one or more of the following flags are available:

**ack**

Filters packets for which the **ack** (acknowledge) flag is set.

**fin**

Filters packets for which the **fin** (finish) flag is set.

**rst**

Filters packets for which the **rst** (reset) flag is set.



<b>sync</b>	Filters packets for which the <b>syn</b> (synchronize) flag is set.
<b>urg</b>	Filters packets for which the <b>urg</b> (urgent) flag is set.
<b>push</b>	Filters packets for which the <b>psh</b> (push) flag is set.
<b>count</b>	Enables statistics for the rule.
<b>log</b>	Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the <b>debug access-list-log buffer</b> command.
<b>mirror</b>	(Supported for rules in ACLs applied on physical interfaces to inbound traffic. Not supported for PBR, rACLs, or ACL-RL.) Mirrors packets matching the rule.
<b>copy-sflow</b>	Sends matching inbound packets to the sFlow collector.

## Modes

ACL configuration mode

## Usage Guidelines

### NOTE

For the current release, filtering by destination address is not supported.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

An IPv6 ACL can only be applied to incoming traffic.

The **hard-drop** keyword is equivalent to the **deny** keyword.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if the double colon were used multiple times. A double colon may not be used to denote an omitted single section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1::2 or 2001:db8::1:1:1:1 are not permitted.)

Although in an extended-ACL rule you can specify **mirror**, **log**, and **copy-sflow**, only one of the three is processed, as follows:

- In a permit rule, the order of precedence is **mirror** > **copy-sflow** > **log**.
- In a deny or hard-drop rule, the order of precedence is **log** > **copy-sflow** > **mirror**.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq seq-value**.
- If you do not know the rule number, type **no** followed by the full syntax except for **seq seq-value**.

## Examples

The following example creates an IPv6 extended ACL, defines a rule for it, and applies the ACL to an interface.

```
device# configure
device(config)# ipv6 access-list extended ip_acl_1
device(conf-ip6acl-ext)# seq 10 deny ipv6 2001:2002:1234:1::/64 2001:1001:1234:1::/64 count
device(conf-ip6acl-ext)# exit
device(config)# interface ethernet 2/5
device(conf-if-eth-2/5)# ipv6 access-group ip_acl_1 in
```

The following example creates an IPv6 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL (rACL).

```
device(config)# ipv6 access-list extended ipv6-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10::1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20::1 count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq bgp count
device(conf-ipacl-ext)# hard-drop tcp host 10::3 host ff02::1 count

device(conf-ipacl-ext)# exit
device(config)# ipv6 receive access-group ipv6-receive-acl-example
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# seq (rules in IPv6 standard ACLs)

Inserts filtering rules in IPv6 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

## Syntax

```
seq seq-value { deny | permit | hard-drop } { any | A:B:C:D:E:F:H:I / prefix_len | host S_IPAddress } [ count ] [ log ] [ copy-
sflow ]
{ deny | permit | hard-drop } { any | A:B:C:D:E:F:H:I / prefix_len | host SIP_address | SIP_addressmask } [ count ] [ log ] [ copy-
sflow ]
no seq seq-value
no { deny | permit | hard-drop } { any | A:B:C:D:E:F:H:I / prefix_len | host SIP_address | SIP_addressmask } [ count ] [ log ]
[ copy-sflow ]
```

## Parameters

### seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

*seq-value*

Valid values range from 1 through 65535.

### permit

Specifies rules to permit traffic.

### deny

Specifies rules to deny traffic.

### hard-drop

Specifies rules to deny traffic.

### any

Specifies all source addresses.

### *S\_IPAddress*

Specify a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

*prefix\_len*

Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

### host

Specifies a source address.

*SIP\_address*

The source address. For options to abbreviate the address, see the Usage Guidelines.

### count

Enables statistics for the rule.

**log**

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

**copy-sflow**

Sends inbound matching packets to the sFlow collector.

## Modes

ACL configuration mode

## Usage Guidelines

This command configures rules to permit or drop traffic based on source addresses. You can also enable counters and either logging or sFlow collection.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

An IPv6 ACL can only be applied to incoming traffic.

The **hard-drop** keyword is equivalent to the **deny** keyword.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if the double colon were used multiple times. A double colon may not be used to denote an omitted single section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1:2 or 2001:db8::1:1:1:1:1 are not permitted.)

Although in a standard-ACL rule you can specify both **log** and **copy-sflow**, only one of the two is processed, as follows:

- In a permit rule, only **copy-sflow** is processed.
- In a deny or hard-drop rule, only **log** is processed.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq seq-value**.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value*.

## Examples

The following example shows how to create an IPv6 standard ACL and define rules for it.

```
device# configure terminal
device(config)# ipv6 access-list standard ipv6-std-acl
device(conf-ip6acl-std)# seq 10 permit host 0:1::1
device(conf-ip6acl-std)# seq 20 deny 0:2::/64
device(conf-ip6acl-std)# seq 30 hard-drop any count
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## seq (rules in MAC extended ACLs)

Inserts filtering rules in a Layer 2 (MAC) extended ACLs. Extended ACLs permit or deny traffic according to source and destination addresses, as well as other parameters.

### Syntax

```
[ seq seq-value ] permit { any | SMAC_address mask | host SMAC_address } { any | host DMAC_address | DMAC_address mask } [ custom-EtherType | arp | cfm | ipv4 | ipv6 | mpls ] [ pcp pcp-match-value ] [ pcp-force out-pcp-value ] [ vlan vlanID ] [ count ] [ log ] [ mirror ] [ copy-sflow ]
```

```
[ seq seq-value ] { deny | hard-drop } { any | SMAC_address mask | host SMAC_address } { any | host DMAC_address | DMAC_address mask } [ custom-EtherType | arp | cfm | ipv4 | ipv6 | mpls ] [ vlan vlanID ] [ pcp pcp-match-value ] [ count ] [ log ] [ mirror ] [ copy-sflow ]
```

```
no seq seq-value
```

```
no [ seq seq-value ] permit { any | SMAC_address mask | host SMAC_address } { any | host DMAC_address | DMAC_address mask } [ custom-EtherType | arp | cfm | ipv4 | ipv6 | mpls ] [ vlan vlanID ] [ pcp pcp-match-value ] [ pcp-force out-pcp-value ] [ count ] [ log ] [ mirror ] [ copy-sflow ]
```

```
no [ seq seq-value ] { deny | hard-drop } { any | SMAC_address mask | host SMAC_address } { any | host DMAC_address | DMAC_address mask } [ custom-EtherType | arp | cfm | ipv4 | ipv6 | mpls ] [ vlan vlanID ] [ pcp pcp-match-value ] [ count ] [ log ] [ mirror ] [ copy-sflow ]
```

### Parameters

#### seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq seq-value**, the rule is added at the end of the list.

*seq-value*

Valid values range from 1 through 65535.

#### permit

Specifies rules to permit traffic.

#### deny

Specifies rules to deny traffic.

#### hard-drop

Specifies rules to deny traffic.

#### any

Specifies all source MAC addresses.

#### SMAC\_address

Specifies a source MAC address and a comparison mask.

*mask*

Specify the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

**host**

Specifies a source MAC address.

*SMAC\_address*

Use the format HHHH.HHHH.HHHH.

**any**

Specifies all destination MAC addresses.

*DMAC\_address*

Specifies a destination MAC address and a comparison mask.

*mask*

Specifies the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

**host**

Specifies a destination MAC address.

*DMAC\_address*

Use the format HHHH.HHHH.HHHH.

*custom-EtherType*

Specifies a custom EtherType value for which to set the permit or deny conditions. Valid values range from 1536 through 65535.

**arp**

Specifies to permit or deny the ARP protocol (0x0806).

**cfm**

Specifies to permit or deny the CFM protocol (0x8902).

**ipv4**

Specifies to permit or deny the IPv4 protocol (0x0800).

**ipv6**

Specifies to permit or deny the IPv6 protocol (0x86dd).

**mpls**

Specifies to permit or deny the MPLS protocol (0x8847).

*vlan vlanID*

Specifies a VLAN interface to which the ACL is bound.

**pcp** *pcp-match-value*

Filters by PCP priority value. Permitted values are 0 through 7.

**pcp-force** *out-pcp-value*

(In **permit** rules applied to incoming traffic) Modifies the PCP priority value to the specified value. Permitted values are 0 through 7.

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

(Currently not supported) (In **permit** rules applied to incoming traffic) Sets the force drop precedence by the specified value. Permitted values are 0 through 2.

**count**

Enables statistics for the rule.

**log**

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

**mirror**

(Supported for rules in ACLs applied on physical interfaces to inbound traffic) Mirrors packets matching the rule.

**copy-sflow**

(Supported for incoming traffic) Sends matching packets to the sFlow collector.

## Modes

ACL configuration mode

## Usage Guidelines

This command configures rules to permit or drop traffic based on source and destination MAC addresses and protocol type. You can also enable counters, logging, mirror, and copy-sflow per rule.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The **hard-drop** keyword is equivalent to the **deny** keyword.

Although in an extended-ACL rule you can specify **mirror**, **log**, and **copy-sflow**, only one of the three is processed, as follows:

- In a permit rule, the order of precedence is **mirror > copy-sflow > log**.
- In a deny or hard-drop rule, the order of precedence is **log > copy-sflow > mirror**.

Support for the **pcp** and **pcp-force** keywords varies with TCAM profile:

**TABLE 1** Support for PCP keywords under TCAM profiles

Keyword	Default	openflow-optimised-1	openflow-optimised-2
<b>pcp</b>	Not supported	Supported	Supported
<b>pcp-force</b>	Not supported	Supported	Not supported

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq seq-value**.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value* .

## Examples

The following example creates a rule in a MAC extended ACL to deny IPv4 traffic from the source MAC address 0022.3333.4444 to the destination MAC address 0022.3333.5555 and to enable the counting of packets.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# seq 100 deny 0022.3333.4444 0022.3333.5555 ipv4 count
```



The following example deletes a rule from a MAC extended ACL.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# no seq 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# seq (rules in MAC standard ACLs)

Inserts filtering rules in Layer 2 (MAC) standard ACLs. Standard ACLs permit or deny traffic according to source address only.

## Syntax

```
seq seq-value { deny | permit | hard-drop } { any | SMAC_address mask | host SMAC_address } [count] [log] [copy-sflow]
{ deny | permit | hard-drop } { any | SMAC_address mask | host SMAC_address } [count] [log] [copy-sflow]
no seq seq-value
no seq { deny | permit | hard-drop } { any | SMAC_address mask | host SMAC_address } [count] [log] [copy-sflow]
```

## Parameters

### seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq seq-value**, the rule is added at the end of the list.

*seq-value*

Valid values range from 1 through 65535.

### permit

Specifies rules to permit traffic.

### deny

Specifies rules to deny traffic.

### hard-drop

Specifies rules to deny traffic.

### any

Specifies all source MAC addresses.

### SMAC\_address

Specifies a source MAC address and a comparison mask.

*mask*

Specify the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask fff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

### host

Specifies a source MAC address.

*SMAC\_address*

Use the format HHHH.HHHH.HHHH.

### count

Enables statistics for the rule.

### log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

**copy-sflow**

Sends matching inbound packets to the sFlow collector.

## Modes

ACL configuration mode

## Usage Guidelines

This command configures rules to permit or drop traffic based on source MAC address. You can also enable counters, logging, and sFlow.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The **hard-drop** keyword is equivalent to the **deny** keyword.

Although in a standard-ACL rule you can specify both **log** and **copy-sflow**, only one of the two is processed, as follows:

- In a permit rule, only **copy-sflow** is processed.
- In a deny or hard-drop rule, only **log** is processed.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq seq-value**.
- If you do not know the rule number, type **no** and then enter the full syntax, without **seq seq-value**.

## Examples

The following command creates statistic-enabled rules in a MAC standard ACL.

```
device# configure terminal
device(config)# mac access-list standard ACL1
device(conf-macl-std)# seq 100 deny host 0022.3333.4444 count
device(conf-macl-std)# seq 110 permit host 0011.3333.5555 count
```

The following command deletes a rule in a MAC standard ACL, by specifying the **seq** number.

```
device# configure terminal
device(config)# mac access-list standard ACL1
device(conf-macl-std)# no seq 100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# service password-encryption

Enables a global password encryption policy that overrides **username** encryption settings.

## Syntax

**service password-encryption**

**no service password-encryption**

## Command Default

Global password encryption policy is enabled.

## Modes

Global configuration mode

## Usage Guidelines

If global password encryption policy is enabled, it overrides **username** encryption settings.

To disable global password encryption policy, enter the **no** form of this command.

Even if global password encryption policy is disabled, the following **username** syntax does encrypt that user's password: **encryption-level 7**.

## Examples

The following example enables global password encryption policy.

```
device# configure terminal
device(config)# service password-encryption
```

The following example disables global password encryption policy.

```
device# configure terminal
device(config)# no service password-encryption
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# service-policy

Binds a policy map to an interface.

## Syntax

```
service-policy in | out policy-mapname  
no service-policy in | out
```

## Command Default

No service policy is created.

## Parameters

**in**  
Binds policy map to inbound traffic.

**out**  
Binds policy map to outbound traffic.

*policy-mapname*  
Name of the policy map.

## Modes

Interface configuration mode

## Usage Guidelines

This command applies a policy-map containing a class-map with specific Policer parameters and match critters to a switch interface. The policy map must be configured before you can apply it (refer to the description of the **policy-map** command).

The **no** form of this command removes the service policy.

## Examples

To create a service policy for outbound traffic on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# service-policy out policymap1
```

To remove a service policy for outbound traffic from a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# no service-policy out
```

To remove a service-policy for inbound traffic on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# no service-policy in
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## session

Configures an LDP session for the neighbor-based filtering of inbound or outbound FECs. You can also configure an authentication key for the LDP session.

### Syntax

```
session remote-ip-addr { filter-fec-in | filter-fec-out prefix-list } | { key string }
```

```
no session remote-ip-addr { filter-fec-in | filter-fec-out } | { key }
```

### Command Default

None

### Parameters

*remote-ip-addr*

Specifies the IP address of the LDP peer.

**filter-fec-in**

Applies neighbor-based LDP FEC filtering on inbound FECs.

**filter-fec-out**

Applies neighbor-based LDP FEC filtering on outbound FECs.

*prefix-list*

Specifies the prefix list for the neighbor to which the filter is applied to allow or prevent the advertisement of FECs.

**key string**

Configures an authentication key on the LDP session. The LDP session can be to an adjacent peer (basic discovery) or to the targeted peer (extended discovery). The string variable specifies a text string of up to 80 characters used for authentication between LDP peers. It must be configured on both peers.

### Modes

MPLS LDP configuration mode

### Usage Guidelines

Use the **no** form of the command to remove the neighbor-based FEC filtering or authentication key from the LDP session.

## Examples

The following example configures LDP to prevent the advertisement of FEC 10.40.40.0/24 through the list-out prefix list and allow all others FECs to neighbor 10.12.12.12.

```
device# configure terminal
device(config)# ip prefix-list list-out deny 10.40.40.0/24
device(config)# ip prefix-list list-out permit 0.0.0.0/0 ge 32
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# session 10.12.12.12 filter-fec-out list-out
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# set-debug

Enables debug configurations for Intermediate System-to-Intermediate System (IS-IS).

## Syntax

**set-debug nsr**

**no set-debug nsr**

## Command Default

Disabled.

## Parameters

**nsr** Specifies nonstop routing (NSR) debugs.

## Modes

IS-IS router configuration mode

## Examples

The following example enables NSR debug configurations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-debug nsr
```

The following example disables NSR debug configurations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no set-debug nsr
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# set extcommunity

Sets an extended BGP community attribute in a route-map instance.

## Syntax

```
set extcommunity { rt extcommunity value | soo extcommunity value }
no set extcommunity
```

## Command Default

No extended BGP community attribute is set.

## Parameters

**rt**

Specifies the route target (RT) extended community attribute.

**soo**

Specifies the site of origin (SOO) extended community attribute.

*extcommunity value*

Specifies the value. The value can be one of the following:

ASN:nn—autonomous-system-number:network-number

Autonomous system (AS) number and network number.

IPAddress:nn—ip-address:network-number

IP address and network number.

## Modes

Route-map configuration mode.

## Usage Guidelines

Enter **no set extcommunity** to delete an extended community set statement from the configuration file.

## Examples

The following example sets the route target to extended community attribute 1:1 for routes that are permitted by the route map.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity rt 1:1
```

The following example sets the site of origin to extended community attribute 2:2 for routes that are permitted by the route map.

```
device# configure terminal
device(config)# ip community-list extended 1 permit 123:2
device(config)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity soo 2:2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# set ip interface null0

Drops traffic when the null 0 statement becomes the active setting as determined by the route-hop selection process for IPv4 policy-based routing.

## Syntax

```
set ip interface null0
no set ip interface null0
```

## Modes

Route-map configuration mode

## Usage Guidelines

The **no** form of this command deletes the matching filter from the ACL.

## Examples

The following example configures the next hop as NULL0 interface to send the traffic to the null interface, thus dropping the packet instead of forwarding it.:

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# set ip interface null0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# set ip next-hop

Sets the IPv4 address of the next hop in a route-map instance.

## Syntax

```
set ip [ global | vrf vrf-name ] next-hop A.B.C.D
```

```
no set ip next-hop A.B.C.D
```

## Parameters

*A.B.C.D*

IPv4 address of the next hop.

**global**

Specifies that the next specified hop address is to be resolved from the global routing table.

**vrf** *vrf-name*

Specifies from which VRF routing table the specified next hop address will be resolved.

**next hop** *A.B.C.D*

Sets the next hop to which to route the packet. The next hop must be adjacent.

## Modes

Route-map configuration mode

## Usage Guidelines

Use the **no** form of this command to delete the matching filter from the ACL.

When a route-map is applied to BGP, and the route-map has multiple **set ip next-hop** statements in a single instance, BGP considers the last **set ip next-hop** in the route-map.

## Examples

The following example configures IPv4 address as the next hop to which the traffic that matches a match statement in the route map must be routed.

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# set ip next-hop 192.168.3.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# set ipv6 interface null0

Drops traffic when the null 0 statement becomes the active setting as determined by the route-hop selection process for IPv6 policy-based routing.

## Syntax

```
set ipv6 interface null0  
no set ipv6 interface null0
```

## Modes

Route-map configuration mode

## Usage Guidelines

The **no** form of this command deletes the matching filter from the ACL.

## Examples

The following example configures the next hop as NULL0 interface to send the traffic to the null interface, thus dropping the packet instead of forwarding it.:

```
device(config)# route-map test-route permit 99  
device(config-route-map-test-route/permit/99)# set ipv6 interface null0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# set ipv6 next-hop

Sets the IPv6 address of the next hop in a route-map instance.

## Syntax

**set ipv6** [ *global* | *vrf vrf-name* ] **next-hop** *AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH*

**no set ipv6 next-hop** *AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH*

## Parameters

*AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH*

IPv6 address of the next hop.

**global**

Specifies that the next specified hop address is to be resolved from the global routing table.

**vrf** *vrf-name*

Specifies from which VRF routing table the specified next hop address will be resolved.

**next hop** *AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH*

Sets the next hop to which to route the packet. The next hop must be adjacent.

## Modes

Route-map configuration mode

## Usage Guidelines

Use the **no** form of this command to delete the matching filter from the ACL.

## Examples

The following example configures IPv6 address as the next hop to which the traffic that matches a match statement in the route map must be routed.

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# set ip next-hop 2001:db8:0:0:0:ff00:42:8329
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# set-overload-bit

Configures a device to signal other devices not to use it as an intermediate hop in their shortest path first (SPF) calculations if the resources of the intermediate system are overloaded and preventing the IS from properly performing Intermediate System-to-Intermediate System (IS-IS) routing.

## Syntax

```

set-overload-bit
set-overload-bit on-startup value
set-overload-bit on-startup wait-for-bgp [ max-bgp-wait-time ]
no set-overload-bit
no set-overload-bit on-startup interval
no set-overload-bit on-startup wait-for-bgp [ max-bgp-wait-time ]

```

## Command Default

A device automatically sets the overload on in its Link State PDUs (LSPs) to other intermediate systems if an overload condition occurs.

## Parameters

### on-startup

Sets the overload bit when the system starts up. The overload bit remains set for the number of seconds configured or until Border Gateway Protocol (BGP) has converged, depending on the subsequent argument or keyword specified.

### *interval*

Specifies the number of seconds the overload bit remains set when the system starts up. Valid values range from 5 through 86400 seconds (24 hours).

### wait-for-bgp

Specifies that the overload bit is set when the system starts up and remains set until BGP has converged.

### *max-bgp-wait-time*

Specifies the maximum time in seconds that IS-IS waits for BGP convergence to complete. When the configured time interval is exceeded without BGP convergence, IS-IS exits the overload state. Valid values range from 5 seconds through 86400 seconds (24 hours). The default is 600 seconds (10 minutes).

## Modes

IS-IS router configuration mode

## Usage Guidelines

The **no** form of the command removes the configured overload state.



## Examples

The following example sets the overload bit to on with immediate effect.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit
```

The following example configures the device to set the overload bit on in all its IS-IS LSPs sent to other ISs during the first five seconds following a successful software reload. After the five seconds expire, the device resets the overload bit to off in all its IS-IS LSPs.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit on-startup 60
```

The following example specifies that the overload bit is set upon system startup and remains set until BGP has converged and specifies that the device that 86400 seconds is the maximum time that IS-IS will wait for BGP convergence to complete.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit on-startup wait-for-bgp 86400
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# sflow enable (global version)

Enables sFlow globally.

## Syntax

**sflow enable**

**no sflow enable**

## Command Default

sFlow is disabled on the system.

## Modes

Global configuration mode

## Usage Guidelines

This command is supported on physical ports only.

The **no** form of this command disable sFlow globally.

## Examples

To enable sFlow globally:

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

# sflow polling-interval (global version)

Configures the polling interval globally.

## Syntax

**sflow polling-interval** *interval\_value*

**no sflow polling-interval**

## Parameters

*interval\_value*

Specifies a value in seconds to set the polling interval. Valid values range from 1 through 65535 seconds.

## Command Default

The default is 20.

## Modes

Global configuration mode

## Usage Guidelines

The interval is the maximum number of seconds between successive samples of counters to be sent to the collector.

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

## Examples

To set the polling interval to 135 seconds:

```
device# configure terminal
device(config)# sflow polling-interval 135
```

# sflow sample-rate (global version)

Sets the number of packets that are skipped before the next sample is taken.

## Syntax

**sflow sample-rate** *samplerate*

**no sflow sample-rate**

## Command Default

The default is 32768.

## Parameters

*samplerate*

Specifies the sampling rate value in packets. Valid values range from 2 through 16777215 packets.

## Modes

Global configuration mode

## Usage Guidelines

Sample-rate is the average number of packets skipped before the sample is taken.

The **no** form of this command restores the default sampling rate.

## Examples

To change the sampling rate to 4096:

```
device# configure terminal
device(config)# sflow sample-rate 4096
```

# shutdown (STP)

Disables Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Per-VLAN Spanning Tree+ (PVST+), or Rapid PVST+ (R-PVST+) globally.

## Syntax

**shutdown**

**no shutdown**

## Command Default

STP is not enabled as it is not required in a loop-free topology.

## Modes

Any of the supported spanning tree configuration modes (STP, RSTP, MSTP, PVST+, R-PVST+)

## Usage Guidelines

Enter **no shutdown** to re-enable any of the supported versions of STP.

## Examples

To disable RSTP globally:

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# shutdown
```

To enable MSTP globally:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# no shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# Show A through Show I

---

## show access-list

For a given network protocol and inbound/outbound direction, displays ACL status information. You can show information for a specified ACL or only for that ACL on a specified interface. You can also display information for all ACLs bound to a specified physical interface, VLAN or VE. You can also display information for receive-path ACLs.

### Syntax

```
show access-list { ip | ipv6 | mac }
show access-list { ip | ipv6 | mac } name { in | out }
show access-list interface { ethernet slot / port | port-channel index | ve vlan_id | vlan vlan_id } { in | out }
show access-list interface management slot / port in
show access-list mac name interface { ethernet slot / port | port-channel index | vlan vlan_id } { in | out }
show access-list mac name management slot / port in
show access-list { ip | ipv6 } name interface { ethernet slot / port | port-channel index | ve vlan_id } { in | out }
show access-list { ip | ipv6 } name interface management slot / port in
show access-list receive { ip | ipv6 }
```

### Parameters

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

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

*name*  
Specifies the ACL name.

**interface**  
Filters by interface.

**ethernet**  
Specifies a physical Ethernet interface.

*slot*  
Specifies a valid slot number.

*port*  
Specifies a valid port number.

**port-channel index**  
Specifies a port-channel interface.

- ve** *vlan\_id*  
Specifies a virtual Ethernet (VE) interface.
- vlan** *vlan\_id*  
Specifies a VLAN interface.
- management** *slot / port*  
Specifies a management interface.
- receive**  
Specifies an ACL that applies to device receive-path traffic.

## Modes

Privileged EXEC mode

## Command Output

The **show access-list** command displays the following information:

Output field	Description
Active	The rule is active and implements the configured action.
Partial	The rule is partially programmed, with the configured action implemented in some cases. This is typically seen for logical interfaces like VLAN, which span multiple hardware resources.
In progress	The rule is currently being programmed into the hardware.
Inactive	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

## Examples

The following example displays the names of IPv4 ACLs applied to the device, interfaces to which they are applied, and the incoming/outgoing direction.

```
device# show access-list ip
Interface Ve 171
  Inbound access-list is not set
  Outbound access-list is IPV4_ACL_000 (From User)
Interface Ethernet 1/2
  Inbound switched access-list is IP_ACL_STD_EXAMPLE (From User)
  Outbound access-list is IP_ACL_EXT_EXAMPLE (From User)
```

The following example displays all interfaces on which an IPv4 ACL is applied in the outgoing direction.

```
device# show access-list ip IPV4_ACL_000 out
ip access-list IPV4_ACL_000 on Ve 171 at Egress (From User)
  seq 10 deny ip host 0.0.0.0 host 10.0.0.0 (Active)
```

The following example displays all interfaces on which an IPv6 ACL is applied in the incoming direction.

```
device# show access-list ipv6 distList in
ipv6 access-list distList on Ethernet 1/4 at Ingress (From User)
  seq 10 deny 2001:125:132:35::/64 (Active)
  seq 20 deny 2001:54:131::/64 (Active)
  seq 30 deny 2001:5409:2004::/64 (Active)
  seq 40 permit any (Active)
```



The following example displays all ACLs applied on a specified interface in the incoming direction.

```
device# show access-list interface ethernet 1/4 in
ipv6 access-list ipv6-std-acl on Ethernet 1/4 at Ingress (From User)
  seq 10 permit host 0:1::1 (Active)
  seq 20 deny 0:2::/64 (Active)
  seq 30 hard-drop any count (Active)
```

The following example displays IPv6 receive-path ACL information.

```
device# show access-list receive ipv6
ipv4 access-list extended ipv6-receive-acl-example
seq 76 deny ip 10.10.95.10 0.0.0.0 any count (Active)

ipv6 access-list extended ipv6-receive-acl-example
seq 10 deny ipv6 3001:2010:145:35::/64 any count (Active)
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show access-list-log buffer

Displays the contents of the log buffer for all ACLs, or for a specified interface.

## Syntax

```
show access-list-log buffer [ interface { ethernet slot / port | port-channel index } ]
```

## Parameters

### interface

Filters by interface.

### ethernet

Specifies a physical Ethernet interface.

#### *slot*

Specifies a valid slot number.

#### *port*

Specifies a valid port number.

### port-channel *index*

Specifies a port-channel interface.

## Modes

Privileged EXEC mode

## Examples

Sample terminal output:

```
device# show access-list-log buffer
Frames Logged on interface 1/2 :
-----
Frame Received Time : Fri Dec 9 3:8:48 2011
Ethernet,          Src : (00:34:56:78:0a:ab), Dst: (00:12:ab:54:67:da)
  Ethtype          : 0x8100
  Vlan tag type    : 0x800
  VlanID           : 0x1
Internet proto, Src : 192.85.1.2, Dst: 192.0.0.1
  Interface       :
  Type of service : 0
  Length          : 110
  Identification  : 0
  Fragmentation   : 00 00
  TTL             : 255
  protocol        : 253
  Checksum        : 39 3a
  Payload type    :
packet(s) repeated : 30
Ingress Deny Logged
-----
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show access-list-log buffer config

Displays the configuration of the ACL buffer.

## Syntax

```
show access-list-log buffer config
```

## Modes

Privileged EXEC mode

## Examples

The following example displays the configuration of the ACL buffer.

```
device# show access-list-log buffer config
ACL Logging is enabled
Buffer exists for interface Eth 2/11
Buffer type is Circular and size is 1000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show access-list overlay transit

Displays which overlay ACL is bound with overlay transit.

## Syntax

```
show access-list overlay transit overlay_transit_name
```

## Parameters

*overlay\_transit\_name*

Specifies the name of the overlay transit.

## Modes

Privileged EXEC mode

## Examples

```
device# show access-list overlay transit tr_name
Overlay Transit Global Binding
  Inbound access-list is abc_ext (From User)
  Outbound access-list is not set
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show access-list overlay type vxlan acl-name

Displays the status of individual filters and binding information of an ACL.

## Syntax

`show access-list overlay type vxlan acl-name user-acl-name`

## Parameters

*user-acl-name*

The overlay VXLAN ACL name.

## Modes

Privileged EXEC mode

## Examples

```
device# show access-list overlay type vxlan acl-name abc_ext
Number of Rules: 4
seq 1000 permit dst-vtep-ip-host 200.1.1.1 src-vtep-ip-host 150.1.1.1 vni 1 vni-mask 0 redirect
Ethernet 2/65 sflow count 44024774(pkts)/52829728800(bytes)
seq 1010 permit dst-vtep-ip-host 200.1.1.2 src-vtep-ip-host 150.1.1.2 vni 2 vni-mask 0 redirect
Ethernet 2/19 sflow count 44024773(pkts)/52829727600(bytes)
seq 1020 permit dst-vtep-ip-host 200.1.1.3 src-vtep-ip-host 150.1.1.3 vni 3 vni-mask 0 redirect
Ethernet 2/43 sflow count 0(pkts)/0(bytes)
seq 1030 permit dst-vtep-ip-host 200.1.1.4 src-vtep-ip-host 150.1.1.4 vni 4 vni-mask 0 redirect
Ethernet 2/67 sflow count 0(pkts)/0(bytes)
Transit : transit_name
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show arp

Displays the address-resolution protocol (ARP) entries.

## Syntax

```
show arp [ summary ] [ vrf name ]  
show arp { ethernet slot / port | ve ve_id } [ vrf name ]  
show arp ip ip-address [ vrf name ]  
show arp [ dynamic | static ] [ summary ] [ vrf name ]
```

## Parameters

### **vrf name**

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

### **ethernet**

Specifies a physical Ethernet interface.

#### *slot*

Specifies a valid slot number.

#### *port*

Specifies a valid port number.

### **ve ve\_id**

Specifies a virtual ethernet (VE) interface.

### **ip ip-address**

Displays the ARP for the specified next-hop IP address.

### **dynamic**

Displays all the dynamic ARP entries in the ARP table.

### **static**

Displays all the static ARP entries in the ARP table.

### **summary**

Displays a summary of the ARP table.

## Modes

Privileged EXEC mode

show arp

## Examples

The following example displays the output of the basic **show arp** command.

```
device# show arp
Address      Mac-address      Interface      MacResolved    Age           Type
-----
11.1.1.20    UnResolved      Eth 3/14      yes            00:00:00     PreArp
12.1.1.20    UnResolved      Ve 10         no             00:00:00     PreArp
11.1.1.111   0610.9427.a001  Eth 3/14      yes            00:01:27     Dynamic
12.1.1.111   0410.9428.0002  Ve 10         yes            00:01:21     Dynamic
11.1.1.141   0000.0011.0141  Eth 3/14      yes            Never         Static
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show bridge-domain

Displays information about Virtual Private LAN Services (VPLS) bridge domains.

## Syntax

```
show bridge-domain [id [ logical-interface [id ] ] ]
```

```
show bridge-domain brief [ { p2mp | p2p } ]
```

```
show bridge-domain vc-peer
```

## Parameters

*id*

Specifies the bridge-domain identifier. The range is from 1 through 4096.

### logical-interface

Causes the display of the ifindex and operational information for logical interfaces configured under the bridge domain.

*id*

Specifies a logical interface instance ID.

### brief

Causes the display of summary bridge-domain information.

### p2mp

Causes the display of multipoint service information.

### p2p

Causes the display of multi-point cross-connect service information.

### vc-peer

Causes the display of summary virtual connection (VC) peer information for the bridge domain.

## Modes

Privileged EXEC mode.

## Usage Guidelines

To display information about all bridge domains, specify the **bridge-domain** option without a bridge-domain identifier.

To display information about all logical interfaces configured under a specific bridge domain, specify the **logical-interface** option without a logical-interface identifier.

## Command Output

The following table describes elements of information displayed in output from the **show bridge-domain** command:

Output field	Description
Assigned LSPs	Assigned label-switched paths.

Output field	Description
AC LIF Count	Number of attachment circuit (AC) logical interfaces in the bridge-domain.
bpdu-drop-enable	Indicates whether dropping Layer 2 (L2) bridge protocol data units (BPDUs) is enabled (TRUE) or disabled (FALSE) for the bridge domain.
Bridge-domain Type	Bridge-domain type. Type can be multipoint service (MP) or multi-point cross-connect (P2P).
Cos Enabled	Indicates whether Cost of Service (CoS) is enabled (True) or disabled (False) for a peer device in the bridge domain.
Load-balance	Indicates whether load balancing is enabled (True) or disabled (False) for a peer device in the bridge domain.
Local switching	Indicates whether local switching is enabled (TRUE) or disabled (FALSE) for the bridge domain.
Local VC lbl	Local virtual connection label (for the pseudowire that corresponds with the peer).
Local MTU	Local maximum transmission unit configuration (for the pseudowire that corresponds with the peer).
Local VC-Type	Local virtual connection mode configuration (for the pseudowire that corresponds with the peer).
Macs Dynamically learned	MAC addresses learned dynamically from traffic on the interface part of the bridge domain.
Macs statically configured	Number of MAC addresses configured statically over interfaces associated with the bridge domain.
Number of configured end-points	Number of endpoints that are configured for the bridge domain.
Number of Active end-points	Number of endpoints that are active in the bridge domain.
PW-profile	Pseudowire profile that is associated the bridge domain.
Remote VC lbl	Remote virtual connection label (for the pseudowire that corresponds with the peer).
Remote VC MTU	Remote maximum transmission unit configuration (for the pseudowire that corresponds with the peer).
Remote VC-Type	Remote virtual connection mode configuration (for the pseudowire that corresponds with the peer).
Total number of VC peers	Number of remote VPLS provider-edge (PE) devices that this node is peered with. (This is the same as the number of remote VPLS peers.)
Total VPLS peers	Number of remote VPLS provider-edge (PE) devices that this node is peered with.
Tunnel cnt	The number of MPLS tunnels that are selected by the pseudowire (corresponding to the peer).
VC id	Virtual connection identifier.
VE if-indx	Routing interface (virtual switching interface) index.
VFI LIF Count:	Number of virtual forwarding interfaces (VFI) in the bridge-domain.

## Examples

The following example shows the information displayed by the **show bridge-domain** command.

```
device# show bridge-domain

Total Number of bridge-domains: 3
Number of bridge-domains: 3

Bridge-domain 1
-----
Bridge-domain Type: mp , VC-ID: 5
Number of configured end-points: 5 , Number of Active end-points: 4
VE if-indx: 1207959555, Local switching: TRUE, bpdu-drop-enable:TRUE
PW-profile: 1, mac-limit: 128000
Number of Mac's learned:90000,      Static-mac count: 10,
VLAN: 100, Tagged ports: 2(2 up), Un-tagged ports: 0 (0 up)
Tagged ports: Eth 0/2/6, eth 0/2/8
Un-tagged ports:

Total PW peers: 2 (2 Operational)
Peer address: 12.12.12.12, State: Operational, Uptime: 2 hr 55 min
    Load-balance: True , Cos enabled:False,
    Assigned LSP;s:
    Tnnl in use: tnl2[RSVP]
    Local VC lbl: 983040, Remote VC lbl: 983040
    Local VC MTU: 1500, Remote VC MTU: 1500,
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 15.15.15.15, State: Operational, Uptime: 2 hr 55 min
    Load-balance: False , Cos enabled:False,
    Assigned LSP's: lsp1, lsp2
    Tnnl in use: tnl1[MPLS]
    Local VC lbl: 983041, Remote VC lbl: 983043
    Local VC MTU: 1500, Remote VC MTU: 1500 ,
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)

Bridge-domain 2
-----
Bridge-domain Type: mp , VC-ID: 100
Number of configured end-points: 5 , Number of Active end-points: 4
VE if-indx: NA, Local switching: FALSE, bpdu-drop-enable:FALSE
PW-profile: profile_1, mac-limit: 262144
Number of Mac's learned:90000,      Static-mac count: 10,
VLAN: 100, Tagged ports: 2(1 up), Un-tagged ports: 0 (0 up)
    Tagged ports: eth 0/2/10, eth 0/1/10
    Un-tagged ports:
VLAN: 150, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
    Tagged ports: eth 0/1/5
    Un-tagged ports:

Bridge-domain 3
-----
Bridge-domain Type: mp , VC-ID: 200
Number of configured end-points: 5 , Number of Active end-points: 4
VE if-indx: 120793855, Local switching: FALSE, bpdu-drop-enable:FALSE
PW-profile: 2, mac-limit: 262144
Number of Mac's learned:90000,      Static-mac count: 10,
Local switching: TRUE,
VLAN: 500, Tagged ports: 2(2 up), Un-tagged ports: 2 (1 up)
Tagged ports:      eth 0/11/6, eth 0/4/3
Un-tagged ports:

Total VPLS peers: 3 (2 Operational)
Peer address: 5.5.5.5, State: Operational, Uptime: 2 hr 35 min
    Load-balance: False , Cos enabled:False,
    Assigned LSP;s:
    Tnnl in use: tnl2[RSVP]
    Local VC lbl: 983050, Remote VC lbl: 983050
    Local VC MTU: 1500,Remote VC MTU: 1500,
    Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 20.20.20.20, State: Operational, Uptime: 0 hr 18 min
```

show bridge-domain

```
    Load-balance: False , Cos enabled:True,
Assigned LSP's:
Tnnl in use: NA,
Local VC lbl: NA, Remote VC lbl: NA
Local VC MTU: 1500,Remote VC MTU: 1500,
Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 10.10.10.10, State: Not-Operational (Tunnel Not Available),
    Load-balance: True , Cos enabled:False,
Assigned LSP's: lsp10, lsp15
Tnnl in use: NA,
Peer Index:2
Local VC lbl: NA, Remote VC lbl: NA
Local VC MTU: 1500,Remote VC MTU: NA ,
Local VC-Type: Ethernet(0x05), Remote VC-Type: NA
```

The following example shows information about a bridge domain (501) in which the **load-balance** and **cos** options are configured for the peer device 10.9.9.9.

```
device# show bridge-domain 501
```

```
Bridge-domain 501
-----
Bridge-domain Type: MP , VC-ID: 501
Number of configured end-points: 2 , Number of Active end-points: 2
VE if-indx: 0, Local switching: TRUE, bpdu-drop-enable: TRUE
PW-profile: default, mac-limit: 0
VLAN: 501, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
Tagged Ports: eth1/6.501
Un-tagged Ports:
Total VPLS peers: 1 (1 Operational):

VC id: 501, Peer address: 10.9.9.9, State: Operational, uptime: 2 min
Load-balance: True , Cos Enabled: True ,
Tunnel cnt: 16
rsvp p101(cos_enable:True cos_value:1)
rsvp p102(cos_enable:True cos_value:1)
rsvp p103(cos_enable:True cos_value:1)
rsvp p104(cos_enable:True cos_value:1)
rsvp p105(cos_enable:True cos_value:1)
rsvp p106(cos_enable:True cos_value:1)
rsvp p107(cos_enable:True cos_value:1)
rsvp p108(cos_enable:True cos_value:1)
rsvp p109(cos_enable:True cos_value:1)
rsvp p110(cos_enable:True cos_value:1)
rsvp p111(cos_enable:True cos_value:1)
rsvp p112(cos_enable:True cos_value:1)
rsvp p113(cos_enable:True cos_value:1)
rsvp p114(cos_enable:True cos_value:1)
rsvp p115(cos_enable:True cos_value:1)
rsvp p116(cos_enable:True cos_value:1)
Assigned LSPs count:0 Assigned LSPs:
Local VC lbl: 989046, Remote VC lbl: 983040,
Local VC MTU: 1500, Remote VC MTU: 1500,
Local VC-Type: 5, Remote VC-Type: 5
```

The following example shows information about bridge domain 501 in which the **load-balance** option, **cos** option and three assigned label-switched paths (p1001, p1002, and p1003) are configured for the peer device 10.9.9.9.

```
device# show bridge-domain 501

Bridge-domain 501
-----
Bridge-domain Type: MP , VC-ID: 501
Number of configured end-points: 2 , Number of Active end-points: 2
VE if-indx: 0, Local switching: TRUE, bpdu-drop-enable: TRUE
PW-profile: default, mac-limit: 0
VLAN: 501, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
Tagged Ports: eth1/6.501
Un-tagged Ports:
Total VPLS peers: 1 (1 Operational):

VC id: 501, Peer address: 10.9.9.9, State: Operational, uptime: 19 sec
  Load-balance: True , Cos Enabled: True ,
  Tunnel cnt: 2
  rsvp p1001(cos_enable:True cos_value:1)
  rsvp p1002(cos_enable:True cos_value:1)
  Assigned LSPs count:3 Assigned LSPs:p1001 p1002 p1000
  Local VC lbl: 989047, Remote VC lbl: 983040,
  Local VC MTU: 1500, Remote VC MTU: 1500,
  Local VC-Type: 5, Remote VC-Type: 5
```

The following example shows the information displayed by the **show bridge-domain brief** command.

```
device# show bridge-domain brief

Total Number of bridge-domains configured: 3
Number of VPLS bridge-domains: 3
Macs Dynamically learned: 100, Macs statically configured: 200

Name      ID(VC-ID)  TYPE    Intf(up)  PWs(up)  macs
-----
1         3000      MP      5(3)      -         5000
2         5000      MP      2(1)      -         80
3         8000      MP      1(1)      3(2)     100000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show cluster

Displays the MCT cluster information including client and member VLAN information.

## Syntax

```
show cluster { cluster-ID [ client [ client-ID ] ] | member vlan
```

## Parameters

*cluster-ID*

Specifies the cluster ID to display the cluster configuration, peer, and client information.

**client**

Specifies the displaying of all clients for the cluster including their names, IDs, local and remote labels, associated interface, and local and remote states.

*client-ID*

Optionally specifies the cluster client ID to also display the associated VLANs and the deployed and undeployed count. However, local and remote label information are not provided..

**member vlan**

Specifies the displaying of the member VLANs for the cluster including the local and remote multicast and unicast labels.

## Modes

Privileged EXEC mode

## Command Output

The **show cluster** command displays the following information:

Output field	Description
Cluster State	Whether the cluster is deployed or undeployed
Client Interfaces Shutdown	Whether local client interfaces are administratively disabled in the cluster to moves all the traffic on the device to remote MCT peer device, resulting in fail-over of traffic to the peer device, as indicated by the FALSE state.
Client Isolation Mode	Client-isolation mode configuration: Strict or Loose
Configured Member Vlan Range	Configured VLANs as members to the MCT cluster.
Active Member Vlan Range	Active member VLANs.
Peer IP	Configured IP address for the MCT cluster peer.
Peer Interface	Configured peer interface slot and port.
Name	Configured client name.
ID	Configured client ID.
ESI	Configured Ethernet Segment ID (ESI) value .
Interface	Configured interface assigned to the client.
Local/Remote State	Local and remote state of the client; Up or Down, Deployed (Dep) or Undeployed (UnDep).

## Examples

The following example shows the information of the cluster on the SLX-OS device.

```
device# show cluster 1

Cluster MCT1 1
=====
Cluster State: Deploy
Client Interfaces Shutdown: FALSE
Client Isolation Mode: Strict
Configured Member Vlan Range: 5, 100-1000
Active Member Vlan Range: 5,200,500-600, 800

Peer Info:
-----
Peer IP: 10.10.10.20, State: Up
Peer Interface: e 1/1

Client Info:
-----
Name      Id   ESI                               interface  Local/Remote State
access1   100 00.a1.b2.c3.d4.e5.f6.89.00       Eth1/8     Up/UP
access2   200 00.11.22.33.44.55.66.77.88       po-chan-2  Dep/UnDep
access3   300 00.24.46.0e.cd.ab.66.16.00       Eth2/3     Up/Down
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# show crypto ca

Displays the crypto trust point/certificate information for HTTPS.

## Syntax

```
show crypto ca {trustpoint | certificates}
```

## Parameters

### trustpoint

Displays the trustpoint and associated key pair details.

### certificates

Displays the CA certificate and Identity certificate details.

## Modes

Privileged EXEC mode

## Usage Guidelines

To execute this command from other configuration modes, use the **do** command modifier.

## Examples

Typical command display output:

```
device# show crypto ca trustpoint
trustpoint: t1; key-pair: k1
```

Typical command display output for certificates:

```
device# show crypto ca certificates
Trustpoint: t1
certificate:
SHA1 Fingerprint=B7:5B:DB:9B:24:69:40:39:36:66:4D:59:2C:69:83:8E:93:CA:23:0C
Subject: C=US, ST=CA, L=SJ, O=BRC, OU=SF, CN=10:00:00:27:F8:87:70:29
Issuer: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Not Before: Oct 6 23:44:27 2014 GMT
Not After : Oct 6 23:44:27 2015 GMT
purposes: sslserver
CA certificate:
SHA1 Fingerprint=76:5B:D4:2C:CB:54:FE:6B:C5:E0:E3:FD:11:B0:88:70:80:12:C6:63
Subject: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Issuer: C=US, ST=CA, L=SJ, O=BR, OU=SF, CN=SOUND/emailAddress=sravi
Not Before: Sep 19 20:56:49 2014 GMT
Not After : Oct 19 20:56:49 2014 GMT
purposes: sslserver
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# show crypto key

Displays the crypto key pair information for HTTPS.

## Syntax

```
show crypto key mypubkey
```

## Modes

Privileged EXEC mode

## Usage Guidelines

To execute this command from other configuration modes, use the **do** command modifier.

## Examples

Typical command output:

```
device# show crypto key mypubkey
key type: ecdsa
key label: k1
key size: 384
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show default threshold

Displays the default thresholds for environmental and alert values for Ethernet interfaces, login, and SFPs.

## Syntax

```
show defaults threshold [ interface type Ethernet | sfp ]
```

## Parameters

### interface type Ethernet

Thresholds for all Ethernet interfaces.

### sfp

Thresholds for the following SFP types:

1GCOP

1 GSR

1 GSR

10 GLR

10 GER

10 GZR

10 GSR

10 GUSR

40GESR

40GLE

40GSR

40GSRINT

100GCLR

100GCWDM

100GLR

100GLRLT

100GPSM

100GSR

QSFP

## Modes

Privileged EXEC mode

## Usage Guidelines

The command works only on SFP type. These thresholds can be changed by means of the **threshold-monitor** command.

## Examples

The following example illustrates default interface sfp thresholds:

```
device# show default threshold sfp
Value for 'type' [1GCOP,1GLR,1GSR,10GER,...]: 1gcop
Type: 1GCOP
-----+-----+-----+-----+-----+-----+-----+
|          |          |          |          |          |          |          |
| Area     |          |          |          |          |          |          |
|          | Value  | Above  | Below  | Value   | Below  | Buffer  |
|          |        | Action | Action |         | Action | Value  |
|          |        |        |        |         |        |        |
| Temp C   |    90  | raslog | none   |    -45  | raslog |    0   |
|          |        |        |        |         |        |        |
| RXP uWatts |  501  | raslog | none   |     6   | raslog |    0   |
|          |        |        |        |         |        |        |
| TXP uWatts |  794  | raslog | none   |    71   | raslog |    0   |
|          |        |        |        |         |        |        |
| Current mA |   45  | raslog | none   |     1   | raslog |    0   |
|          |        |        |        |         |        |        |
| Voltage mV | 3700  | raslog | none   |   2900  | raslog |    0   |
|          |        |        |        |         |        |        |
-----+-----+-----+-----+-----+-----+-----+
device#
```

# show dot1x

Displays 802.1X-related information.

## Syntax

```
show dot1x [ all ]
```

```
show dot1x [ interface ethernet slot/port]
```

```
show dot1x [ diagnostics | session-info | statistics ] { interface ethernet slot/port }
```

## Parameters

### all

Displays detailed dot1x information for all of the ports.

### interface

Displays the state of a specified interface.

### diagnostics

Displays diagnostics information for the authenticator associated with a port.

### session-info

Displays all statistical information of an established session.

### statistics

Displays the statistics of a specified interface.

## Modes

Privileged EXEC mode

## Examples

The following example shows the overall state of 802.1X authentication on the system.

```
device# show dot1x
802.1X Port-Based Authentication: Enabled
PAE Capability:                    Authenticator Only
Protocol Version:                  2
Auth Server:                       RADIUS
Readiness test timeout:            10
RADIUS Configuration
-----
Position:                          1
Server Address:                     10.24.65.6
Port:                               1812
Secret:                             xxxxxxxxxx
Retry Interval:                     5 seconds
```

```
show dot1x
```

The following example shows detailed 802.1X authentication information for all of the ports.

```
device# show dot1x all
802.1X Port-Based Authentication: Enabled
PAE Capability:                      Authenticator Only
Protocol Version:                    2
Auth Server:                         RADIUS
Readiness test timeout:              10

RADIUS Configuration
-----
Position:                            1
Server Address:                      10.20.106.144
Port:                                 1812
Secret:                              testing123
Retry Interval:                      4 seconds

Position:                            2
Server Address:                      10.20.106.189
Port:                                 1812
Secret:                              testing123
Retry Interval:                      4 seconds

802.1X info for interface Eth 1/31
-----
Port Control:                        Auto
Protocol Version:                    2
ReAuthentication:                    Enabled
Auth Fail Max Attempts:              0
ReAuth Max:                          2
Tx Period:                          30 seconds
Quiet Period:                        60 seconds
Supplicant Timeout:                 30 seconds
Re-Auth Interval:                   3600 seconds
Dynamic VLAN assigned:               50
Filter-strict-security:              Enabled
IP ACL assigned (IN|OUT):             IPEXT-50 | IPEXT-OUT-50
MAC ACL assigned:                    mac-ext
```

The following example shows all diagnostics information for the authenticator associated with a port.

```
device# show dot1x diagnostics interface ethernet 1/2
802.1X Diagnostics for interface Eth 1/2
-----
authEnterConnecting:                 1
authEaplogoffWhileConnecting:        0
authEnterAuthenticating:             1
authSuccessWhileAuthenticating:      1
authTimeoutWhileAuthenticating:      0
authFailWhileAuthenticating:         0
authEapstartWhileAuthenticating:     0
authEaplogoffWhileAuthenticating:    0
authReauthsWhileAuthenticated:       0
authEapstartWhileAuthenticated:      0
authEaplogoffWhileAuthenticated:     0
BackendResponses:                    11
BackendAccessChallenges:             10
BackendOtherrequestToSupplicant:     11
BackendAuthSuccess:                  1
BackendAuthFails:                    0
```

The following example shows state of a specified interface.

```
device# show dot1x interface ethernet 1/31
802.1X info for interface Eth 1/31
-----
Port Control:           Auto
Protocol Version:      2
ReAuthentication:      Enabled
Auth Fail Max Attempts: 0
ReAuth Max:            2
Tx Period:             30 seconds
Quiet Period:          60 seconds
Supplicant Timeout:    30 seconds
Re-Auth Interval:      3600 seconds
Dynamic VLAN assigned: 50
Filter-strict-security: Enabled
IP ACL assigned (IN|OUT): IPEXT-50 | IPEXT-OUT-50
MAC ACL assigned:      mac-ext
```

The following example shows information for all clients on the port.

```
device# show dot1x session-info interface ethernet 1/2
802.1X Session info for interface Eth 1/2
-----
Mac Address: 0021.5ec6.15ce
-----
User Name:             md5user2
Session Time:          2 secs
Terminate Cause:       Not terminated yet
Session Status:        Authorized
PAE State:             Authenticated
BE State:              Idle
VLAN:                  N/A
IP ACL (IN | OUT):     N/A | N/A
MAC ACL:               N/A
Current Id:            18
Id From Server:        17
```

The following example shows the statistics of a specified interface.

```
device# show dot1x statistics interface ethernet 1/2
802.1X statistics for interface Eth 1/2
-----
EAPOL Frames Rx:      12
EAPOL Frames Tx:      43
EAPOL Start Frames Rx: 1
EAPOL Logoff Frames Rx: 0
EAP Rsp/Id Frames Rx: 1
EAP Response Frames Rx: 10
EAP Req/Id Frames Tx: 23
EAP Request Frames Tx: 10
Invalid EAPOL Frames Rx: 0
EAPOL Length Error Frames Rx: 0
EAPOL Last Frame Version Rx: 1
Invalid EAP Frames Rx: 0
EAP Length Error Frames Rx: 0
EAPOL Last Frame Src: 0021.5ec6.15ce
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show event-handler activations

Displays operational data of activated event-handlers.

## Syntax

**show event-handler activations**

## Modes

Privileged EXEC mode

## Command Output

The **show event-handler activations** command displays the following information:

Output field	Description
Event-handler	Displays the event-handler name.
Last Trigger Activation Time	Displays the time of the last trigger activation. If no trigger was activated, displays "Never".
Total Trigger Activations	Displays the total number of trigger activations.
Last Action Completion Time	Displays the completion time of the last event-handler action run. If no event-handler action ran, displays "Never".
Last Action Completion Status. Exit Code =	Displays the status of the last completed event-handler action. If the Python script assigns exit codes, such codes are displayed here. An exit code of 0 indicates one of the following: <ul style="list-style-type: none"> <li>No code was assigned to this condition.</li> <li>The script author assigned 0 to a specified condition.</li> </ul>
Total Action Completions	Displays the number of completed event-handler actions.

## Examples

The following example displays event-handler operational data.

```
device# show event-handler activations

Event-handler : evh1
Last Trigger Activation Time: 2015-04-30 17:28:12
Total Trigger Activations: 25
Last Action Completion Time: 2015-04-30 17:28:57
Last Action Completion Status: Exit Code = 0
Total Action Completions: 25

Event-handler : evh2
Last Trigger Activation Time: 2015-04-28 22:02:51
Total Trigger Activations: 8
Last Action Completion Time: 2015-04-28 22:02:58
Last Action Completion Status: Exit Code = 0
Total Action Completions: 8
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# show file

Displays the contents of a file in the local flash memory.

## Syntax

```
show file filename
```

## Parameters

*filename*

The name of the file to be displayed.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is supported only on the local device.

## Examples

The following example displays the contents of a file in the flash memory.

```
device# show file defaultconfig.cluster
vlan dot1q tag native
!
cee-map default
remap fabric-priority priority 0
remap lossless-priority priority 0
priority-group-table 15.0 pfc off
priority-group-table 1 weight 40 pfc on
priority-group-table 2 weight 60 pfc off
priority-table 2 2 2 1 2 2 2 15.0
!!
port-profile default
vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
!
interface Port-channel 1
vlag ignore-split
  description Homerun port-channel on MM1
  shutdown
!
interface Port-channel 2
  vlag ignore-split
  description Homerun port-channel on MM2
  shutdown
!
protocol lldp
!!
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging auditlog class SECURITY
!
end
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ha

Displays the High Availability (HA) status of the management modules.

## Syntax

```
show ha
```

## Modes

Privileged EXEC mode

## Usage Guidelines

When a failover occurs while the management modules are not synchronized, the standby management module reboots, and the failover is disruptive.

## Examples

To display HA status:

```
device# show ha
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# show hardware port-group

Displays the port groups and their ports for the SLX 9850 36x100G line cards.

## Syntax

```
show hardware port-group
```

## Modes

Privileged EXEC mode

## Command Output

The **show hardware port-group** command displays the following information:

Output field	Description
Port-Group	Port group number.
Port	Port numbers for the port group.

## Examples

The following example displays the port groups and their ports.

```
device# show hardware port-group
Port-Group          Port
=====
3/1                 3/1 ,2 ,3 ,4 ,5 ,6 ,7 ,26 ,27 ,28
3/2                 3/8 ,9 ,10 ,11 ,12 ,13 ,29 ,30 ,31 ,32
3/3                 3/15 ,16 ,17 ,18 ,19 ,20 ,14 ,33 ,34 ,35
3/4                 3/41 ,42 ,43 ,44 ,45 ,46 ,21 ,22 ,23 ,24
3/5                 3/48 ,49 ,50 ,51 ,52 ,53 ,25 ,36 ,47 ,54
3/6                 3/55 ,56 ,57 ,58 ,59 ,60 ,37 ,38 ,39 ,40
```

\* Only the first six ports in each group are 100g capable ports

## History

Release version	Command history
16r.1.00	This command was introduced.

# show interface stats brief

Displays a brief list of interface statistics.

## Syntax

```
show interface stats brief [ slot line_card_number ]
```

## Parameters

### slot

The slot.

*line\_card\_number*

The line card number.

## Modes

Privileged exec mode

## Examples

Follow this example to display brief interface statistics for a specific line card.

```
device# show interface stats brief slot 2
```

Interface	Packets		Error		Discards		CRC
	rx	tx	rx	tx	rx	tx	
Eth 2/1	44127	38570	0	0	0	0	0
Eth 2/2	0	0	0	0	0	0	0
Eth 2/3	37319	38572	0	0	0	0	0
Eth 2/4	0	0	0	0	0	0	0
Eth 2/5	37319	38853	0	0	0	0	0
Eth 2/6	0	0	0	0	0	0	0
Eth 2/7	0	0	0	0	0	0	0
Eth 2/8	0	0	0	0	0	0	0
Eth 2/9	4735	6859	0	0	0	0	0
Eth 2/10	37319	45808	0	0	0	0	0
Eth 2/11	290725948	22923725	0	0	0	0	0
Eth 2/12	0	0	0	0	0	0	0
Eth 2/13	3395530417	37764	0	0	0	0	0
Eth 2/14	0	0	0	0	0	0	0
Eth 2/15	0	0	0	0	0	0	0
Eth 2/16	0	0	0	0	0	0	0
Eth 2/17	0	0	0	0	0	0	0
Eth 2/18	0	0	0	0	0	0	0
Eth 2/19	0	0	0	0	0	0	0
Eth 2/20	0	0	0	0	0	0	0
...							
Eth 2/57	559837487	20446529	0	0	0	0	0
Eth 2/58	37315	39887	0	0	0	0	0
Eth 2/59	37313	38567	0	0	0	0	0
Eth 2/60	15046998	38571	0	0	0	0	0
Eth 2/61	162123590	38566	0	0	0	0	0
Eth 2/62	164529088	3095486	0	0	0	0	0
Eth 2/63	42510	38570	0	0	0	0	0
Eth 2/64	37312	47235	0	0	0	0	0
Eth 2/65	0	0	0	0	0	0	0
Eth 2/66	2023	3289	0	0	0	0	0
Eth 2/67	365498908	37764	0	0	0	0	0

## History

Release version	Command history
16r.1.00	This command was introduced.

# show interface stats detail

Displays a detailed list of interface statistics.

## Syntax

```
show interface stats detail [ interface { ethernet slot/port | port-channel port_channel_number } | slot line_card_number ]
```

## Parameters

### interface

Specifies what type of interface is to be displayed

### ethernet

Specifies an Ethernet interface.

*slot/port*

The Ethernet slot and port .

### port-channel

Specifies a port channel interface.

*port\_channel\_number*

The port channel number. Depending on the platform the number ranges from 1 to 512.

### slot

The slot.

*line\_card\_number*

The line card number.

## Modes

Privileged exec mode





# show access-list overlay transit

Displays which overlay ACL is bound with overlay transit.

## Syntax

`show access-list overlay transit overlay_transit_name`

## Parameters

*overlay\_transit\_name*

Specifies the name of the overlay transit.

## Modes

Privileged EXEC mode

## Examples

```
device# show access-list overlay transit tr_name
Overlay Transit Global Binding
  Inbound access-list is abc_ext (From User)
  Outbound access-list is not set
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp

Displays BGP4 route information.

## Syntax

```
show ip bgp ip-addr [ /prefix ]
```

```
show ip bgp { ip-addr [ /prefix ] } [ longer-prefixes | vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of a neighbor in dotted-decimal notation, with optional mask.

*/prefix*

IPv4 mask length in CIDR notation.

**longer-prefixes**

Filters on prefixes equal to or greater than that specified by *prefix*.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays sample output from the **show ip bgp** command.

```
device# show ip bgp
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp attribute-entries

Displays BGP4 route-attribute entries that are stored in device memory.

## Syntax

```
show ip bgp attribute-entries [ vrf vrf-name ]
```

## Parameters

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

The route-attribute entries table lists the sets of BGP4 attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4 route-attribute entries that are stored in device memory.

## Examples

This example show sample output for the **show ip bgp attribute-entries** command.

```
device# show ip bgp attribute-entries
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp dampened-paths

Displays all BGP4 dampened routes..

## Syntax

```
show ip bgp dampened-paths [ vrf vrf-name ]
```

## Parameters

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the **show ip bgp dampened-paths** command.

```
device# show ip bgp dampened-paths

      Status Code  >:best d:damped h:history *:valid
      Network      From      Flaps Since      Reuse      Path
*d 110.110.114.0/24 160.160.160.10 38    0 :3 :49    0 :10:10   111
*d 110.110.113.0/24 160.160.160.10 38    0 :3 :49    0 :10:10   111
*d 110.110.112.0/24 160.160.160.10 38    0 :3 :49    0 :10:10   111
*d 110.110.111.0/24 160.160.160.10 38    0 :3 :49    0 :10:10   111
*d 110.110.110.0/24 160.160.160.10 38    0 :3 :49    0 :10:10   111
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp filtered-routes

Displays BGP4 filtered routes that are received from a neighbor or peer group.

## Syntax

```
show ip bgp filtered-routes [ detail ] [ ip-addr { / mask } [ longer-prefixes ] ] [ as-path-access-list name ] | prefix-list name ]
[ vrf vrf-name ]
```

## Parameters

### detail

Optionally displays detailed route information.

### ip-addr

IPv4 address of the destination network in dotted-decimal notation.

### mask

(Optional) IPv4 mask of the destination network in CIDR notation.

### longer-prefixes

Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

### as-path-access-list name

Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

### prefix-list name

Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

### vrf vrf-name

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays BGP4 filtered routes.

```
device# show ip bgp filtered-routes 10.11.12.13 prefix-list myprefixlist
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp flap-statistics

Displays BGP4 route-dampening statistics for all dampened routes with a variety of options.

## Syntax

```
show ip bgp flap-statistics
show ip bgp flap-statistics ip-addr { / mask } [ longer-prefixes [ vrf vrf-name ] | vrf vrf-name ]
show ip bgp flap-statistics neighbor ip-addr [ vrf vrf-name ]
show ip bgp flap-statistics regular-expression name [ vrf vrf-name ]
show ip bgp flap-statistics vrf vrf-name
```

## Parameters

*ip-addr*

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

*mask*

IPv4 mask of a specified route in CIDR notation.

**longer-prefixes**

Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

**vrf** *vrf-name*

Specifies a VRF instance.

**neighbor**

Displays flap statistics only for routes learned from the specified neighbor.

*ip-addr*

IPv4 address of the neighbor.

**regular-expression**

Specifies a regular expression in the display output on which to filter.

*name*

Name of an AS-path filter or regular expression.

## Modes

Privileged EXEC mode

## Examples

This example displays flap statistics for a neighbor.

```
device# show ip bgp flap-statistics neighbor 10.11.12.13
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# 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 [ vrf vrf-name ]  
show ip bgp neighbors routes-summary [ vrf vrf-name ]  
show ip bgp neighbors vrf vrf-name
```

## Parameters

*ip-addr*  
IPv4 address of a neighbor in dotted-decimal notation.

**last-packet-with-error**  
Displays the last packet with an error.

**route-summary**  
Displays routes received, routes accepted, number of routes advertised by peer, and so on.

**vrf** *vrf-name*  
Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to view configuration information and statistics for BGP4 neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

## Examples

This example shows sample output from the show ip bgp neighbors command.

```

device# show ip bgp neighbors

Total number of BGP Neighbors: 2

1  IP Address: 123.123.123.3, AS: 333 (EBGP), RouterID: 9.9.9.9, VRF: default-vrf
   State: ESTABLISHED, Time: 0h1m32s, KeepAliveTime: 60, HoldTime: 180
     KeepAliveTimer Expire in 17 seconds, HoldTimer Expire in 147 seconds
   Minimal Route Advertisement Interval: 0 seconds
     RefreshCapability: Received
   Messages:      Open      Update      KeepAlive      Notification      Refresh-Req
     Sent       : 2         15         3339           1                 0
     Received: 2         0          3356           0                 0
   Last Update Time: NLRI                               Withdraw        NLRI              Withdraw
                   Tx: 0h1m32s                         ---              Rx: ---           ---
   Last Connection Reset Reason: User Reset Peer Session
   Notification Sent:      Cease/Administrative Reset
   Notification Received: Unspecified
   Neighbor NLRI Negotiation:
     Peer configured for IPV4 unicast Routes
   Neighbor ipv6 MPLS Label Capability Negotiation:
   Neighbor AS4 Capability Negotiation:
   Outbound Policy Group:
     ID: 2, Use Count: 2
   BFD: Disabled
     Byte Sent: 146, Received: 0
     Local host: 123.123.123.2, Local Port: 44575
     Remote host: 123.123.123.3, Remote Port: 179

2  IP Address: 160.160.160.10, AS: 111 (EBGP), RouterID: 193.24.0.1, VRF: default-vrf
   State: ESTABLISHED, Time: 0h1m33s, KeepAliveTime: 30, HoldTime: 90
     KeepAliveTimer Expire in 12 seconds, HoldTimer Expire in 86 seconds
   Minimal Route Advertisement Interval: 0 seconds
     RefreshCapability: Received
   Messages:      Open      Update      KeepAlive      Notification      Refresh-Req
     Sent       : 8         0          553            5                 0
     Received: 8         9          498            0                 0
   Last Update Time: NLRI                               Withdraw        NLRI              Withdraw
                   Tx: ---                               ---              Rx: 0h1m33s      ---
   Last Connection Reset Reason: User Reset Peer Session
   Notification Sent:      Cease/Administrative Reset
   Notification Received: Unspecified
   Neighbor NLRI Negotiation:
     Peer configured for IPV4 unicast Routes
   Neighbor ipv6 MPLS Label Capability Negotiation:
   Neighbor AS4 Capability Negotiation:
   Outbound Policy Group:
     ID: 2, Use Count: 2
   BFD: Disabled
     Byte Sent: 121, Received: 0
     Local host: 160.160.160.20, Local Port: 53791
     Remote host: 160.160.160.10, Remote Port: 179

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp neighbors advertised-routes

Displays the routes that the device has advertised to the neighbor during the current BGP4 session.

## Syntax

```
show ip bgp neighbors ip-addr advertised-routes [ detail | / mask-bits ] [ vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of a neighbor in dotted-decimal notation.

**detail**

Displays details of advertised routes.

*mask-bits*

Number of mask bits in CIDR notation.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays the details of advertised routes.

```
device# show ip bgp neighbors 123.123.123.3 advertised-routes

      There are 5 routes advertised to neighbor 123.123.123.3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
Prefix      Next Hop      MED      LocPrf      Weight      Status
1  110.110.110.0/24  123.123.123.2    0
   AS_PATH: 222 111
2  110.110.111.0/24  123.123.123.2    0
   AS_PATH: 222 111
3  110.110.112.0/24  123.123.123.2    0
   AS_PATH: 222 111
4  110.110.113.0/24  123.123.123.2    0
   AS_PATH: 222 111
5  110.110.114.0/24  123.123.123.2    0
   AS_PATH: 222 111
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp neighbors flap-statistics

Displays the route flap statistics for routes received from or sent to a BGP4 neighbor.

## Syntax

```
show ip bgp neighbors ip-addr flap-statistics [ vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of a neighbor in dotted-decimal notation.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example shows flap statistics.

```
device#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp neighbors last-packet-with-error

Displays information about the last packet that contained an error from any of a device's neighbors.

## Syntax

```
show ip bgp neighbors ipv6-addr last-packet-with-error [ decode ] [ vrf vrf-name ]
```

## Parameters

*ip-addr*

IP address of a neighbor in dotted-decimal notation.

**decode**

Decodes last packet that contained an error from any of a device's neighbors.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example shows sample output from the **show ip bgp neighbors last-packet-with-error** command when no packet from a specified neighbor contained an error.

```
device# show ip bgp neighbors 123.123.123.3 last-packet-with-error
```

```
Received Message Length: 45
BGP Message:
 0xffffffff 0xffffffff 0xffffffff 0xffffffff 0x002d0104
 0x014b00b4 0x09090909 0x10020601 0x04010000 0x01020202
 0x00020280 0x00
```

```
BGP Header
Marker: 0xffffffff 0xffffffff 0xffffffff 0xffffffff
Message Length: (0x002d) 45
Message Type: (0x01) OPEN
```

```
OPEN Message
Version: (0x04) 4
AS Number: (0x014b) 331
Hold Time: (0x00b4) 180
BGP Identifier: (0x09090909) 9.9.9.9
Optional Parameter length: (0x10) 16
```

```
OPEN message optional parameters
Parameter Type: (0x02) Capability
Parameter Length: (0x06) 6
  Capability Type: (0x01) MULTIPROTOCOL EXTENSIONS
  Capability Length: (0x04) 4
  AFI: (0x0100) Unknown(256)
  Reserved: (0x00) 0
  SAFI: (0x01) Unicast
```

```
Parameter Type: (0x02) Capability
Parameter Length: (0x02) 2
  Capability Type: (0x02) ROUTE REFRESH(new)
  Capability Length: (0x00) 0
```

```
Parameter Type: (0x02) Capability
Parameter Length: (0x02) 2
  Capability Type: (0x80) ROUTE REFRESH(old)
  Capability Length: (0x00) 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

## Syntax

```
show ip bgp neighbors ip-addr received
show ip bgp neighbors ip-addr received detail [ vrf vrf-name ]
show ip bgp neighbors ip-addr received prefix-filter [ vrf vrf-name ]
show ip bgp neighbors ip-addr vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of a neighbor in dotted-decimal notation.

**detail**

Displays detailed information for ORFs received from BGP4 neighbors of the device.

**vrf** *vrf-name*

Specifies a VRF instance.

**prefix-filter**

Displays the results for ORFs that are prefix-based.

## Modes

Privileged EXEC mode

## Examples

This example displays .

```
device# show ip bgp neighbors 10.5.5.6 received prefix-filter
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp neighbors received-routes

Lists all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

## Syntax

```
show ip bgp neighbors ip-addr received-routes [ detail ] [ vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of a neighbor in dotted-decimal notation.

**detail**

Displays detailed route information.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays output for the **show ip bgp neighbors received-routes** command.

```
device# show ip bgp neighbors 160.160.160.10 received-routes

      There are 5 received routes from neighbor 160.160.160.10
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
      E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
      S:SUPPRESSED F:FILTERED s:STALE
      Prefix          Next Hop          MED           LocPrf        Weight Status
  1    110.110.110.0/24  160.160.160.10    0             100           0      BE
      AS_PATH: 111
  2    110.110.111.0/24  160.160.160.10    0             100           0      BE
      AS_PATH: 111
  3    110.110.112.0/24  160.160.160.10    0             100           0      BE
      AS_PATH: 111
  4    110.110.113.0/24  160.160.160.10    0             100           0      BE
      AS_PATH: 111
  5    110.110.114.0/24  160.160.160.10    0             100           0      BE
      AS_PATH: 111
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip bgp neighbors rib-out-routes

Displays information about BGP4 outbound RIB routes.

## Syntax

```
show ip bgp neighbors ipaddr rib-out-routes ip-addr mask [ vrf vrf-name ]
show ip bgp neighbors ip-addr rib-out-routes detail ip-addr mask [ vrf vrf-name ]
show ip bgp neighbors ip-addr rib-out-routes detail [ vrf vrf-name ]
show ip bgp neighbors ip-addr rib-out-routes [ vrf vrf-name ]
```

## Parameters

*ip-addr*  
IP address of a neighbor in dotted-decimal notation.

**vrf** *vrf-name*  
Specifies a VRF instance.

**detail**  
Displays detailed RIB route information.

## Modes

Privileged EXEC mode

## Examples

This example shows sample output from the **show ip bgp neighbors rib-out-routes** command.

```
device# show ip bgp neighbors 123.123.123.3 rib-out-routes

      There are 5 RIB_out routes for neighbor 123.123.123.3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
Prefix      Next Hop      MED      LocPrf      Weight      Status
1      110.110.110.0/24  160.160.160.10  0           100         0          BE
      AS_PATH: 111
2      110.110.111.0/24  160.160.160.10  0           100         0          BE
      AS_PATH: 111
3      110.110.112.0/24  160.160.160.10  0           100         0          BE
      AS_PATH: 111
4      110.110.113.0/24  160.160.160.10  0           100         0          BE
      AS_PATH: 111
5      110.110.114.0/24  160.160.160.10  0           100         0          BE
      AS_PATH: 111
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4 neighbors.

## Syntax

```
show ip bgp neighbors ip-addr routes
```

```
show ip bgp neighbors ip-addr routes { best | not-installed-best | unreachable } [ vrf vrf-name ]
```

```
show ip bgp neighbors ip-addr routes detail { best | not-installed-best | unreachable } [ vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of a neighbor in dotted-decimal notation.

**best**

Displays routes received from the neighbor that are the best BGP4 routes to their destination.

**not-installed-best**

Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in the route table because the device received better routes from other sources.

**unreachable**

Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example displays

```
device# show ip bgp neighbors 10.11.12.13 routes best vrf red
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4 neighbors.

## Syntax

```
show ip bgp neighbors ip-addr routes-summary [ vrf vrf-name ]
```

## Parameters

*ip-addr*

IPv4 address of a neighbor in dotted-decimal notation.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example displays route summary information received in UPDATE messages.

```
device# show ip bgp neighbors routes-summary
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp peer-group

Displays peer-group information.

## Syntax

```
show ip bgp peer-group peer-group-name [ vrf vrf-name ]
```

## Parameters

*peer-group-name*

Specifies a peer group name.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Only the parameters that have values different from their defaults are listed.

## Examples

This example shows sample output from the **show ip bgp peer-group** command.

```
device# show ip bgp peer-group
1  BGP peer-group is pg
   Address family : IPV4 Unicast
   activate
   Address family : IPV6 Unicast
   no activate
   Members:
   IP Address: 1.1.1.1, AS: 100
   IP Address: 1::1, AS: 100

2  BGP peer-group is pg6
   Address family : IPV4 Unicast
   activate
   Address family : IPV6 Unicast
   no activate
   Currently there are no members
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp routes

Displays BGP4 route information that is filtered by the table entry at which the display starts.

## Syntax

```
show ip bgp routes [ num | ip-address/prefix | age num | as-path-access-list name | best | cidr-only | community-access-list
name | community-reg-expression expression | detail | local | neighbor ip-addr | nexthop ip-addr | no-best | not-
installed-best | prefix-list string | regular-expression name | route-map name | summary | unreachable ] [ vrf vrf-name ]
```

## Parameters

*num*

Table entry at which the display starts.

*ip-address/prefix*

Table entry at which the display starts.

**age**

Displays BGP4 route information that is filtered by age.

**as-path-access-list** *name*

Displays BGP4 route information that is filtered by autonomous system (AS)-path access control list (ACL). The name must be between 1 and 32 ASCII characters in length.

**best**

Displays BGP4 route information that the device selected as best routes.

**cidr-only**

Displays BGP4 routes whose network masks do not match their class network length.

**community-access-list** *name*

Displays BGP4 route information for an AS-path community access list. The name must be between 1 and 32 ASCII characters in length.

**community-reg-expression** *expression*

Displays BGP4 route information for an ordered community-list regular expression.

**detail**

Displays BGP4 detailed route information.

**local**

Displays BGP4 route information about selected local routes.

**neighbor** *ip-addr*

Displays BGP4 route information about selected BGP neighbors.

**nexthop** *ip-addr*

Displays BGP4 route information about routes that are received from the specified next hop.

**no-best**

Displays BGP4 route information that the device selected as not best routes.

**not-installed-best**

Displays BGP4 route information about best routes that are not installed.

**prefix-list** *string*

Displays BGP4 route information that is filtered by prefix list. The string must be between 1 and 32 ASCII characters in length.

**regular-expression** *name*

Displays BGP4 route information about routes that are associated with the specified regular expression.

**route-map** *name*

Displays BGP4 route information about routes that use the specified route map.

**summary**

Displays BGP4 summary route information.

**unreachable**

Displays BGP4 route information about routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example shows sample input from the **show ip bgp routes** command when an IP address is specified.

```
device# show ip bgp routes 50.55.55.10

Number of BGP Routes matching display condition : 8
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
S:SUPPRESSED F:FILTERED s:STALE
Prefix      Next Hop      MED      LocPrf      Weight      Status
1  10.55.55.0/24  16.1.1.1      0          100          0          BME
   AS_PATH: 65200 65100
2  10.55.55.0/24  17.1.1.1      0          100          0          ME
   AS_PATH: 65200 65100
3  10.55.55.0/24  19.1.1.1      0          100          0          mE
   AS_PATH: 65200 65100
4  10.55.55.0/24  21.1.1.1      0          100          0          mE
   AS_PATH: 65200 65100
5  10.55.55.0/24  18.1.1.1      0          100          0          mE
   AS_PATH: 65200 65100
6  10.55.55.0/24  22.1.1.1      0          100          0          mE
   AS_PATH: 65200 65100
7  10.55.55.0/24  23.1.1.1      0          100          0          mE
   AS_PATH: 65200 65100
8  10.55.55.0/24  20.1.1.1      0          100          0          mE
   AS_PATH: 65200 65100
Last update to IP routing table: 0h28m14s      Route is advertised to 7 peers:
17.1.1.1(65200)                                18.1.1.1(65200)
19.1.1.1(65200)                                20.1.1.1(65200)
20.1.1.1(65200)                                21.1.1.1(65200)
22.1.1.1(65200)
23.1.1.1(65200)
```

This example shows sample input from the **show ip bgp routes summary** command.

```
device# show ip bgp routes summary

Total number of BGP routes (NLRIs) Installed      : 1
Distinct BGP destination networks                 : 1
Filtered bgp routes for soft reconfig             : 0
Routes originated by this router                  : 1
Routes selected as BEST routes                    : 1
Routes Installed as BEST routes                   : 1
BEST routes not installed in IP forwarding table  : 0
Unreachable routes (no IGP route for NEXTHOP)    : 0
IBGP routes selected as best routes               : 0
EBGP routes selected as best routes               : 0
BEST routes not valid for IP forwarding table     : 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip bgp routes community

Displays BGP4 route information that is filtered by community and other options.

## Syntax

```
show ip bgp routes community { num | internet | local-as | no-advertise | no-export } [ vrf vrf-name ]
```

## Parameters

### community

Displays routes filtered by a variety of communities.

### *num*

Specific community member.

### internet

Displays routes for the Internet community.

### local-as

Displays routes for a local sub-AS within the confederation.

### no-advertise

Displays routes with this community that cannot be advertised to any other BGP4 devices at all.

### no-export

Displays routes for the community of sub-ASs within a confederation.

### vrf *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows output from the **show ip bgp routes community** command when the **internet** keyword is used.

```
device# show ip bgp routes community internet
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip bgp summary

Displays BGP information such as the local autonomous system number (ASN), maximum number of routes supported, and some BGP4 statistics.

## Syntax

```
show ip bgp summary [ vrf vrf-name ]
```

## Parameters

**vrf vrf-name**  
Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays summary BGP information.

```
device# show ip bgp summary

BGP4 Summary
Router ID: 4.4.4.4   Local AS Number: 65300
Confederation Identifier: not configured
Confederation Peers:
Maximum Number of IP ECMP Paths Supported for Load Sharing: 2
Number of Neighbors Configured: 8, UP: 8
Number of Routes Installed: 80088, Uses 7688448 bytes
Number of Routes Advertising to All Neighbors: 70077 (10011 entries), Uses 600660 bytes
Number of Attribute Entries Installed: 16, Uses 1664 bytes
Neighbor Address  AS#      State    Time      Rt:Accepted  Filtered  Sent      ToSend
16.1.1.1         65200    ESTAB    2h26m 8s  10011       0         1         0
17.1.1.1         65200    ESTAB    2h26m 8s  10011       0        10010     0
18.1.1.1         65200    ESTAB    2h26m 7s  10011       0        10011     0
19.1.1.1         65200    ESTAB    2h26m 7s  10011       0        10011     0
20.1.1.1         65200    ESTAB    2h26m 7s  10011       0        10011     0
21.1.1.1         65200    ESTAB    2h26m 7s  10011       0        10011     0
22.1.1.1         65200    ESTAB    2h26m 2s  10011       0        10011     0
23.1.1.1         65200    ESTAB    2h26m 7s  10011       0        10011     0
...
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip dhcp relay address interface

Displays IP DHCP relay addresses configured on supported interfaces.

## Syntax

```
show ip dhcp relay address interface [ ethernet slot/port | ve interface number ]
```

## Parameters

**ethernet** slot/port

Interface name in slot/port format.

**ve** interface number

Interface name in slot/port format.

## Modes

Privileged EXEC mode

## Examples

The following example displays DHCP relay address(es) configured on interface 1/4:

```
device# show ip dhcp relay address interface ethernet 1/4
-----
Interface                Relay Address                VRF Name
-----
Eth 1/4                  10.3.4.5                     blue
Eth 1/4                  10.5.1.1                     default-vrf
```

The following example displays DHCP relay address(es) configured on Ve 300:

```
device# show ip dhcp rel add int ve 300
-----
Interface                Relay Address                VRF Name
-----
Ve 300                   10.0.1.2                     default-vrf
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip dhcp relay gateway

Displays IP DHCP Relay gateway addresses.

## Syntax

```
show ip dhcp relay gateway [interface [ ethernet slot/port | Ve number ]]
```

## Parameters

*interface*

The interface ethernet slot/port number or the Ve number.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display the gateway address configured on the switch or on the interface.

## Examples

To display the gateway address configured on the switch:

```
device# show ip dhcp relay gateway
-----
Interface                Gateway Address
-----
Eth 3/5                  10.1.1.1
Ve 100                   100.1.1.1
```

To display the gateway address configured on the interface:

```
device# show ip dhcp relay gateway interface ethernet 3/5
-----
Interface                Gateway Address
-----
Eth 3/5                  10.1.1.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip dhcp relay statistics

Displays the general information about the DHCP Relay function.

## Syntax

```
show ip dhcp relay statistics
```

## Modes

Privileged EXEC mode

## Usage Guidelines

The **show ip dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on the switch:

- DHCP Server IP Address configured in the switch.
- Number of DHCP DISCOVERY, OFFER, REQUEST, ACK, NAK, DECLINE, and RELEASE packets received.
- Number of DHCP client packets received (on port 67) and relayed by the Relay Agent.
- Number of DHCP server packets received (on port 67) and relayed by the Relay Agent.

DHCP unicast packets are forwarded directly per route. These packets are not trapped to the management module. As a result, the DHCP renewal Request/ACK and DHCP Release packets are not be counted toward statistics.

## Examples

To display general information about the DHCP relay function:

```
device# show ip dhcp relay statistics
DHCP Relay Statistics:
-----
Address          Disc.    Offer    Req.     Ack      Nak      Decline  Inform
-----
10.1.0.1         400     100     2972    2968     0        0         0
20.2.0.1         400     100     2979    2975     0        0         0
30.3.0.1         400     100     3003    2998     0        0         0
40.4.0.1         400     100     3026    3018     0        0         0

Client Packets: 12780
Server Packets: 12359
Client Packets Dropped: 0
Server Packets Dropped: 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip igmp groups

Displays information related to learned groups in the IGMP protocol module.

## Syntax

```
show ip igmp groups [ detail | interface | vlan vlan_id ]
```

## Parameters

### detail

Displays detailed information.

### interface

Specifies an interface type.

### vlan *vlan\_id*

Specifies a VLAN interface.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display the IGMP database, including configured entries for either all groups on all interfaces, or all groups on specific interfaces, or specific groups on specific interfaces.

## Examples

The following example displays the IP IGMP groups.

```
device# show ip igmp groups
Total Number of Groups: 2
IGMP Connected Group Membership
Group Address  Interface Uptime      Expires      Last Reporter  Version
225.1.1.1      vlan25   00:05:27    00:02:32    25.1.1.1202
Member Ports: eth 2/24
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip igmp interface

Displays Layer 3 IGMP interface configuration information.

## Syntax

```
show ip igmp interface [ ethernet slot/port | port-channel | Ve ]
```

## Modes

Privileged EXEC mode

## Examples

The following example displays IGMP protocol information for port-channel 1.

```
device# show ip igmp interface port-channel 1
Interface po1
IGMP disabled
```

The following example displays the output for the **show ip igmp interface** command.

```
device# show ip igmp interface
Interface Ve100
IGMP enabled
IGMP query interval 30 seconds
IGMP other-querierinterval 65 seconds
IGMP query response time 10 seconds
IGMP last-member query interval 1 seconds
IGMP immediate-leave disabled
IGMP querier100.0.0.1(this system)
IGMP version 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip igmp snooping

Displays IGMP snooping information.

## Syntax

```
show ip igmp snooping [mrouter vlan vlan_id | vlan vlan_id]
```

## Parameters

**mrouter vlan** *vlan\_id*

Specifies which VLAN interface to display the mrouter configuration related information.

**vlan** *vlan\_id*

Specifies which VLAN interface to display the snooping configuration related information.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use the **show ip igmp snooping** command to display IGMP snooping information, display multicast router port related information for the specified VLAN, or to display snooping statistics for the specified VLAN in the IGMP protocol module.

## Examples

The following example displays IGMP snooping information.

```
device# show ip igmp snooping vlan 45
Vlan ID: 45
Multicast Router ports:  eth3/2
Querier - Enabled,
IGMP Operation mode: IGMPv2
Is Fast-Leave Enabled : Disabled
Max Response time = 10
Last Member Query Interval = 1
Query interval = 125
Number of Multicast Groups: 1
Group: 225.0.0.1
Member Ports:  eth4/22 eth6/15
Mapped MAC address: 0100.5e00.0001
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip igmp ssm-map

Displays the association between a configured prefix list and source address mapped to it.

## Syntax

```
show ip igmp ssm-map
```

## Modes

Privileged EXEC mode

## Usage Guidelines

## Command Output

The **show ip igmp ssm-map** command displays the following information:

Output field	Description
PrefixList Name	The name assigned to the prefix list.
Source Address	The source address IP.

## Examples

The following example shows the association between a configured prefix list and source address mapped to it.

```
device# show ip igmp ssm-map
```

```
+-----+-----+
| PrefixList Name | Source Address |
+-----+-----+
| ssm-map-230-to-232 | 203.0.0.10 |
| ssm-map-233-to-234 | 204.0.0.11 |
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip igmp statistics vlan

Displays information for a specific VLAN.

## Syntax

```
show ip igmp statistics vlan vlan-id
```

## Parameters

*vlan-id*

Specifies the VLAN-ID. The range is 1 through 4090.

## Modes

Privileged EXEC mode

## Examples

The following example displays the IP IGMP statistics on VLAN 1.

```
device# show ip igmp statistics interface vlan 1

IGMP packet statistics for all interfaces in vlan 1:
IGMP Message type      Edge-Received   Edge-Sent   Edge-Rx-Errors   ISL Received
Membership Query       0               0           0                 0
V1 Membership Report   0               0           0                 0
V2 Membership Report   0               0           0                 0
Group Leave            0               0           0                 0
V3 Membership Report   0               0           0                 0
PIM hello              0               0           0                 0

IGMP Error Statistics:
Unknown types          0
Bad Length             0
Bad Checksum           0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip igmp statistics interface

Displays IGMP statistics for an interface.

## Syntax

```
show ip igmp statistics interface [ ethernet slot/port | port-channel | ve ve interface ID ]
```

## Parameters

**ethernet** slot/port

Represents an Ethernet interface name in slot/port format.

**port-channel** number

Specifies a port-channel interface. The range is from 1 through 64.

**ve** Ve interface number

Specifies a virtual Ethernet (VE) interface number. The range is 1 - 4096.

## Modes

Privileged EXEC mode

## Examples

The following example displays the output of the **show ip igmp statistics interface** command.

```
device# show ip igmp statistics interface ve100
IGMP packet statistics for ve100:
IGMP Message type      Edge-Received  Edge-Sent  Edge-Rx-Errors
Membership Query        0             229        0
V1 Membership Report    0             0          0
V2 Membership Report    0             0          0
Group Leave             0             0          0
V3 Membership Report    0             0          0
PIM hello               456           0          0

IGMP Error Statistics:
Unknown types           0
Bad Length              0
Bad Checksum            0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip interface

Displays the IP address, status, and configuration for a specified interface.

## Syntax

```
show ip interface { brief | ethernet slot/port | loopback number | ve vlan-id }
```

## Parameters

### **brief**

Specifies a brief summary of IP interface status and configuration.

### **ethernet** *slot/port*

Specifies an Ethernet slot and port.

### **loopback** *number*

Specifies a loopback interface. Valid values range from 1 through 255.

### **ve** *vlan-id*

Specifies a virtual Ethernet (VE) interface.

## Modes

Privileged EXEC mode

## Usage Guidelines

You can also display a brief summary of such information for all interfaces.

## Examples

The following example displays information about all of the interfaces in the summary format.

```
device# show ip interface brief
```

Interface	IP-Address	Vrf	Status	Protocol
=====	=====	=====	=====	=====
Port-channel 1	unassigned		administratively down	down
Port-channel 2	unassigned		administratively down	down
Port-channel 7	unassigned		up	up
Loopback 1	1.2.3.4	default-vrf	up	up
Ethernet 1/1	unassigned	default-vrf	administratively down	down
Ethernet 1/2	unassigned	default-vrf	up	up
Ve 7	19.19.19.1	default-vrf	up	up

The following example displays the IP interface status of a specified Ethernet port.

```
device# show ip interface ethernet 1/1
Ethernet 1/1 is up protocol is up
Primary Internet Address is 10.0.0.4/24 broadcast is 10.0.0.255
IP MTU is 1500
Proxy Arp is Enabled
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
Vrf : default-vrf
```

The following example displays the IP interface status of a loopback interface.

```
device# show ip interface loopback 1
Loopback 1 is up protocol is up
Primary Internet Address is 1.2.3.4/32
IP MTU is 1500
Proxy Arp is not Enabled
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
Vrf : default-vrf
```

The following example displays the IP interface status of a VE interface.

```
device# show ip int ve 10
Ve 10 is up protocol is down
Vlan is 10
Hardware is Virtual Ethernet, address is 609c.9f00.2e87
Current address is 609c.9f00.2e87
Interface index (ifindex) is 1207959562
Primary Internet Address is 100.0.0.1/24 broadcast is 100.0.0.255
IP MTU is 1500
Proxy Arp is Enabled
Vrf : default-vrf
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip multicast snooping

Displays IP multicast snooping configuration information.

## Syntax

```
show ip multicast snooping [ mcachevlan interface | vlan vlan-id ]
```

## Parameters

### mcache

Specifies the multicast cache entries.

### vlan interface

Specifies which VLAN's snooping mcache entries should be displayed.

### vlan

Specifies the VLAN.

### vlan-id

Specifies the VLAN-ID.

## Modes

User EXEC mode

## Usage Guidelines

## Examples

The following example displays the output for the **show ip multicast snooping mcache** command.

```
device# show ip multicast snooping mcache
Flags : V2|V3 : IGMP Receiver, P_G : PIM (*,G) Join, P_SG: PIM (S,G) Join
VlanID : 25
-----
1(*, 225.1.1.1 )00:02:15NumOIF: 1
Outgoing Ports:
eth2/24      Flags: 0x14 ( V2)  00:02:15/126s
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf

Displays OSPF information.

## Syntax

```
show ip ospf [ vrf name ]
```

## Parameters

**vrf name**

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the show ip ospf command.

```
device# show ip ospf
OSPF Version                Version 2
Router Id                   10.0.0.4
ASBR Status                 No
ABR Status                  No          (0)
Redistribute Ext Routes from
Initial SPF schedule delay  0          (msecs)
Minimum hold time for SPF  0          (msecs)
Maximum hold time for SPF  0          (msecs)
External LSA Counter        0
External LSA Checksum Sum   0
Originate New LSA Counter  0
Rx New LSA Counter         0
External LSA Limit          14913080
Administrative Distance
- External Routes:         110
- Intra Area Routes:       110
- Inter Area Routes:       110
Database Overflow Interval  0
Database Overflow State :  NOT OVERFLOWED
RFC 1583 Compatibility :   Disabled
NSSA Translator:           Enabled
Nonstop Routing:           Disabled
Graceful Restart           Enabled
Graceful Restart Helper    Enabled
Graceful Restart Time      120
LDP-SYNC: Not globally enabled
Interfaces with LDP-SYNC enabled:
None
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf area

Displays the OSPF area table in a specified format.

## Syntax

```
show ip ospf area { A.B.C.D | decimal } database link-state [ adv-router router-id | advertise index | asbr { asbr-id | adv-router router-id } | extensive | link-state-id id | network { net-id | adv-router router-id } | nssa { nssa-id | adv-router router-id } | router { router-id | adv-router router-id } | self-originate | sequence-number num | summary { id | adv-router router-id } ] [ vrf vrfname ]
```

```
show ip ospf area [ vrf vrfname ]
```

## Parameters

*A.B.C.D*

Area address in dotted decimal format.

*decimal*

Area address in decimal format. Valid values range from 0 to 2147483647.

**database link-state**

Displays database link-state information.

**adv-router** *router-id*

Displays the link state for the advertising router that you specify.

**advertise** *index*

Displays the link state by Link State Advertisement (LSA) index.

**asbr**

Displays the link state for all autonomous system boundary router (ASBR) links.

*asbr-id*

Displays the state of a single ASBR link that you specify.

**extensive**

Displays detailed information for all entries in the OSPF database.

**link-state-id** *id*

Displays the link state by link-state ID.

**network**

Displays the link state by network link.

*net-id*

Displays the link state of a particular network link that you specify.

**nssa**

Displays the link state by not-so-stubby area (NSSA).

*nssa-id*

Displays the link state of a particular NSAA area that you specify.

**router**

Displays the link state by router link.

*router-id*

Displays the link state of a particular router link that you specify.

**self-originate**

Displays self-originated link states.

**sequence-number** *num*

Displays the link-state by sequence number that you specify.

**summary**

Displays the link state summary. Can specify link-state ID or advertising router ID.

*id*

Displays the link state for the advertising router that you specify.

**vrf vrf name**

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Examples

The following example shows output for the **show ip ospf area** command.

```
device# show ip ospf area
```

```
Number of Areas is 1
```

Index	Area	Type	Cost	SPFR	ABR	ASBR	LSA	Checksum (Hex)
1	0	normal	0	4305	0	0	5	00024f5a

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip ospf border-routers

Displays information about border routers and boundary routers.

## Syntax

```
show ip ospf border-routers [ A.B.C.D ] [ vrf vrfname ]
```

## Parameters

*A.B.C.D*

Specifies the router ID in dotted decimal format.

**vrf** *vrf name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display information about area border routers (ABRs) and autonomous system boundary routers (ASBRs). You can display information for all ABRs and ASBRs or for a specific router.

## Examples

The following example displays information for all ABRs and ASBRs:

```
device# show ip ospf border-routers
```

# show ip ospf config

Displays OSPF information.

## Syntax

```
show ip ospf config [ vrf name ]
```

## Parameters

**vrf name**

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the show ip ospf config command.

```
device# show ip ospf config

Router OSPF: Enabled
Nonstop Routing: Disabled
Graceful Restart: Enabled
Graceful Restart Helper: Enabled
Graceful Restart Time: 120

Redistribution: Disabled
Default OSPF Metric: 10
Maximum Paths: 8
OSPF Auto-cost Reference Bandwidth: Disabled
Default Passive Interface: Disabled
OSPF Redistribution Metric: Type2
OSPF External LSA Limit: 14913080
OSPF Database Overflow Interval: 0
RFC 1583 Compatibility: Disabled
VRF Lite capability: Disabled
Router id: 10.0.0.4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf database

Shows OSPFv2 database information.

## Syntax

```
show ip ospf database database-summary [ vrf vrfname ]
show ip ospf database external-link-state [ advertise index | extensive | link-state-id id | router-id router-id | sequence-number num ] [ vrf vrfname ]
show ip ospf database grace-link-state [ vrf vrfname ]
show ip ospf database link-state [ adv-router router-id | advertise index | asbr { asbr-id | adv-router router-id } | extensive | link-state-id id | network { net-id | adv-router router-id } | nssa { nssa-id | adv-router router-id } | router { router-id | adv-router router-id } | self-originate | sequence-number num | summary { id | adv-router router-id } ] [ vrf vrfname ]
show ip ospf database [ [ vrf vrfname ]
```

## Parameters

### database-summary

Displays how many link state advertisements (LSAs) of each type exist for each area, as well as total number of LSAs.

### vrf name

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

### external-link-state

Displays information by external link state, based on the following parameters:

#### advertise index

Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's External LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

#### extensive

Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

#### link-state-id id

Displays external LSAs for the LSA source that you specify.

#### router-id router-id

Displays external LSAs for the advertising router that you specify.

#### sequence-number num

Displays the External LSA entries for the hexadecimal LSA sequence number that you specify.

### link-state

Displays the link state, based on the following parameters:

#### adv-router router-id

Displays the link state for the advertising router that you specify.

**advertise** *index*

Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's external-LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

**asbr**

Displays autonomous system boundary router (ASBR) LSAs.

**extensive**

Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

**link-state-id** *id*

Displays LSAs for the LSA source that you specify.

**network**

Displays either all network LSAs or the LSAs for a network that you specify.

**nssa**

Displays either all NSSA LSAs or the LSAs for a not-so-stubby area (NSSA) that you specify.

**router**

Displays LSAs by router link.

**router-id** *router-id*

Displays LSAs for the advertising router that you specify.

**self-originate**

Displays self-originated LSAs.

**sequence-number**

Displays the LSA entries for the hexadecimal LSA sequence number that you specify.

**summary**

Displays summary information. You can specify link-state ID or advertising router ID.

**adv-router** *router-id*

Displays the link state for the advertising router that you specify.

## Modes

Privileged EXEC mode

## Examples

The following example shows output for the **show ip ospf database** command.

```
device# show ip ospf database
```

```
Link States
```

Index	Area ID	Type	LS ID	Adv Rtr	Seq (Hex)	Age	Cksum
1	0	Rtr	200.1.2.3	200.1.2.3	0x80000bb8	235	0x6a51
2	0	Rtr	20.20.20.20	20.20.20.20	0x80000088	1680	0xcb6a
3	0	Rtr	54.1.1.1	54.1.1.1	0x8000009f	599	0x6c3d
4	0	Net	53.1.1.1	200.1.2.3	0x80000006	235	0xd22
5	0	Net	53.54.43.53	200.1.2.3	0x8000007e	626	0x53e6

The following example shows output for the **show ip ospf database** command when the **database-summary** keyword is used.

```
device# show ip ospf database database-summary
```

Area ID	Router	Network	Sum-Net	Sum-ASBR	NSSA-Ext	Opq-Area	Subtotal
0	3	2	0	0	0	0	5
AS External							0
Total	3	2	0	0	0	0	5

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf filtered-lsa area

Displays information about type3 LSA filters attached to specified OSPFv2 areas and lists LSAs filtered in or out.

## Syntax

```
show ip ospf filtered-lsa area { ip-address | decimal } { in | out } [ vrf vrf-name ]
```

## Parameters

*ip-address*

Specifies the IP address of an area.

*decimal*

Specifies an area address in decimal format. Valid values range from 0 through 2147483647.

**in**

Specifies the incoming direction.

**out**

Specifies the outgoing direction.

**vrf** *vrf-name*

Specifies the name of the VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example displays information about type 3 LSA filtering in the out direction for OSPFv2 area 0.

```
device# show ip ospf filtered-lsa area 0 out
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf interface

Displays information about all or specific OSPF-enabled interfaces.

## Syntax

```
show ip ospf interface [ A.B.C.D | brief ] [ vrf vrf-name ]
```

```
show ip ospf interface [ ethernet slot/port | loopback number | ve vlan_id ] [ brief ] [ vrf vrf-name ]
```

```
show ip ospf interface [ vrf vrf-name ]
```

## Parameters

*A.B.C.D*

Specifies interface IP address in dotted decimal format.

**brief**

Displays summary information.

**vrf** *vrf-name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

**ethernet** *slot/port*

Specifies an Ethernet slot and port.

**loopback** *number*

Specifies a loopback port number. Valid values range from 1 through 255.

**ve** *vlan\_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096

## Modes

Privileged EXEC mode

## Examples

The following example displays OSPF information about all enabled interfaces.

```
device# show ip ospf interface

Ethernet 1/2 admin up, oper up
  IP Address 53.1.1.36, Area 0
  BFD is disabled
  Database Filter: Not Configured
  State BDR, Pri 1, Cost 1, Options -----E-, Type broadcast Events 3
  Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
  DR: Router ID 200.1.2.3      Interface Address 53.1.1.1
  BDR: Router ID 20.20.20.20  Interface Address 53.1.1.36
  Neighbor Count = 1, Adjacent Neighbor Count= 1
  Neighbor:      53.1.1.1 [id 200.1.2.3] (DR)
  Authentication-Key: None
  MD5 Authentication: Key None, Key-Id None , Auth-change-wait-time 300
  LDP-SYNC: Disabled, State: -

Loopback 1 admin up, oper up
  IP Address 20.20.20.20, Area 0
  BFD is disabled
  Database Filter: Not Configured
  State DR, Pri 1, Cost 1, Options -----E-, Type broadcast Events 2
  Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
  DR: Router ID 20.20.20.20  Interface Address 20.20.20.20
  BDR: Router ID 0.0.0.0     Interface Address 0.0.0.0
  Neighbor Count = 0, Adjacent Neighbor Count= 0
  Authentication-Key: None
  MD5 Authentication: Key None, Key-Id None , Auth-change-wait-time 300
  LDP-SYNC: Disabled, State: -
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip ospf neighbor

Displays OSPF neighbor information.

## Syntax

```
show ip ospf neighbor [ extensive ] [ ethernet slot/port | router-id A.B.C.D | ve vlan_id ] [ vrf vrf-name ]
show ip ospf neighbor [ vrf vrf-name ]
```

## Parameters

### extensive

Displays detailed neighbor information.

### ethernet slot/port

Specifies an Ethernet slot and port.

### router-id A.B.C.D

Displays neighbor information for the specified router ID (in dotted decimal format).

### ve vlan\_id

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

### vrf vrf-name

Specifies the name of the VRF instance. If this option is not used, details for the default VRF instance are shown in the output.

## Modes

Privileged EXEC mode

## Examples

The following example displays information about OSPF neighbors.

```
device# show ip ospf neighbor
```

```
Number of Neighbors is 1, in FULL state 1
```

Port	Address	Pri	State	Neigh Address	Neigh ID	Ev	Opt	Cnt
Eth 1/2	53.1.1.36	1	FULL/DR	53.1.1.1	200.1.2.3	6	66	0

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf redistribute route

Displays routes that have been redistributed into OSPF.

## Syntax

```
show ip ospf redistribute route [ A.B.C.D:M ] [ [ vrf vrfname ] ]
```

## Parameters

*A.B.C.D:M*

Specifies an IP address and mask for the output.

*vrf vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output for the **show ip ospf redistribute route** command.

```
device# show ip ospf redistribute route
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf routes

Displays OSPF calculated routes.

## Syntax

```
show ip ospf routes [ A.B.C.D ] [ vrf vrfname ]
```

## Parameters

*A.B.C.D*

Specifies a destination IP address in dotted decimal format.

vrf *vrfname*

Specifies the name of the VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display routes that OSPF calculated. You can display all routes or you can display information about a specific route.

## Examples

The following example displays all OSPF-calculated routes.

```
device# show ip ospf routes
```

```
OSPF Regular Routes 7:
```

```

Destination      Mask          Path_Cost  Type2_Cost Path_Type
1.1.1.1          255.255.255.255 1          0          Intra
Adv_Router      Link_State   Dest_Type  State      Tag        Flags
1.1.1.1          1.1.1.1     Network    Valid      0          6
Paths Out_Port  Next_Hop    Type       State
1   Lo 1        0.0.0.0    OSPF      0 0

Destination      Mask          Path_Cost  Type2_Cost Path_Type
1.1.1.2          255.255.255.255 1          0          Intra
Adv_Router      Link_State   Dest_Type  State      Tag        Flags
1.1.1.1          1.1.1.1     Network    Valid      0          6
Paths Out_Port  Next_Hop    Type       State
1   Lo 2        0.0.0.0    OSPF      0 0

Destination      Mask          Path_Cost  Type2_Cost Path_Type
1.1.1.3          255.255.255.255 1          0          Intra
Adv_Router      Link_State   Dest_Type  State      Tag        Flags
1.1.1.1          1.1.1.1     Network    Valid      0          6
Paths Out_Port  Next_Hop    Type       State
1   Lo 3        0.0.0.0    OSPF      0 0

Destination      Mask          Path_Cost  Type2_Cost Path_Type
1.1.1.4          255.255.255.255 1          0          Intra
Adv_Router      Link_State   Dest_Type  State      Tag        Flags
1.1.1.1          1.1.1.1     Network    Valid      0          6
Paths Out_Port  Next_Hop    Type       State
1   Lo 4        0.0.0.0    OSPF      0 0

Destination      Mask          Path_Cost  Type2_Cost Path_Type
1.1.1.5          255.255.255.255 1          0          Intra
Adv_Router      Link_State   Dest_Type  State      Tag        Flags
1.1.1.1          1.1.1.1     Network    Valid      0          6
Paths Out_Port  Next_Hop    Type       State
1   Lo 5        0.0.0.0    OSPF      0 0

Destination      Mask          Path_Cost  Type2_Cost Path_Type
1.1.1.6          255.255.255.255 1          0          Intra
Adv_Router      Link_State   Dest_Type  State      Tag        Flags
1.1.1.1          1.1.1.1     Network    Valid      0          6
Paths Out_Port  Next_Hop    Type       State
1   Lo 6        0.0.0.0    OSPF      0 0

Destination      Mask          Path_Cost  Type2_Cost Path_Type
1.1.1.7          255.255.255.255 1          0          Intra
Adv_Router      Link_State   Dest_Type  State      Tag        Flags
1.1.1.1          1.1.1.1     Network    Valid      0          6
Paths Out_Port  Next_Hop    Type       State
1   Lo 7        0.0.0.0    OSPF      0 0

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf summary

Displays summary information for all OSPF instances.

## Syntax

```
show ip ospf summary [ vrf vrfname ]
```

## Parameters

**vrf** *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Examples

```
device# show ip ospf summary
```

```
Seq Instance      Intfs  Nbrs  Nbrs-Full LSAs  Routes
1  default-vrf    5      2     1         12      2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf traffic

Displays OSPF traffic details.

## Syntax

```
show ip ospf traffic
```

```
show ip ospf traffic [ ethernet slot/port | loopback number | ve vlan_id] [ vrf vrf-name ]
```

## Parameters

### interface

Specifies an interface.

### ethernet *slot / port*

Specifies an Ethernet slot and port.

### loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

### ve *vlan\_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

### vrf *vrf-name*

Specifies the name of the VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display details of OSPF traffic sent and received. You can display all traffic or specify a particular interface.

## Examples

The following example shows all OSPF traffic.

```
device# show ip ospf traffic

                Packets Received          Packets Sent
Hello                10                    10
Database             90                    89
LSA Req              12                    11
LSA Upd              12                    12
LSA Ack              12                    12
No Packet Errors!
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip ospf virtual link

Displays information about virtual links.

## Syntax

```
show ip ospf virtual link [ index ] [ vrf vrfname ]
```

## Parameters

*index*

Shows information about all virtual links or one virtual link that you specify.

*vrf vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Examples

The following example shows information about all virtual links.

```
device# show ip ospf virtual link
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip ospf virtual neighbor

Displays information about virtual neighbors.

## Syntax

```
show ip ospf virtual neighbor [ index ] [ [ vrf vrfname ] ]
```

## Parameters

*index*

Shows information about all virtual neighbors or one virtual neighbor that you specify.

*vrf vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

## Modes

Privileged EXEC mode

## Examples

The following example shows information about all virtual neighbors:

```
device# show ip ospf virtual neighbor
```

# show ip pim bsr

Displays bootstrap router (BSR) information.

## Syntax

```
show ip pim [ all-vrf | vrf vrf-name ] bsr
```

## Parameters

### all-vrf

Displays information for all VRFs.

### vrf *vrf-name*

Displays information for a specific VRF instance.

### bsr

Displays BSR information.

## Modes

User EXEC mode

## Usage Guidelines

When entered without the **vrf** option, this command displays information for the default VRF instance.

## Command Output

The **show ip pim bsr** command displays the following information:

Output Field.	Description
BSR address	The IP address of the interface configured as the PIM Sparse BSR.
BSR priority	The priority assigned to the interface for use during the BSR election process. During BSR election, the priorities of the candidate BSRs are compared and the interface with the highest BSR priority becomes the BSR.
Hash mask length	The number of significant bits in the IP multicast group comparison mask. This mask determines the IP multicast group numbers for which the device can be a BSR. The default is 32 bits, which allows the device to be a BSR for any valid IP multicast group number.  <b>NOTE</b> This field appears only if this device is a candidate BSR.
Next bootstrap message in	Indicates how much time will pass before the BSR sends the next bootstrap message. The time is displayed in "hh:mm:ss" format.

Output Field.	Description
	<p><b>NOTE</b> This field appears only if this device is the BSR.</p>
Next Candidate-RP-advertisement message in	<p>Indicates how much time will pass before the BSR sends the next candidate PR advertisement message. The time is displayed in "hh:mm:ss" format.</p> <p><b>NOTE</b> This field appears only if this device is a candidate BSR.</p>
RP	<p>Indicates the IP address of the Rendezvous Point (RP).</p> <p><b>NOTE</b> This field appears only if this device is a candidate BSR.</p>
group prefixes	<p>Indicates the multicast groups for which the RP listed by the previous field is a candidate RP.</p> <p><b>NOTE</b> This field appears only if this device is a candidate BSR.</p>
Candidate-RP-advertisement period	<p>Indicates how frequently the BSR sends candidate RP advertisement messages.</p> <p><b>NOTE</b> This field appears only if this device is a candidate BSR.</p>

## Examples

The following example shows information for a device that has been elected as the BSR.

```
device> show ip pim bsr
PIMv2 Bootstrap information
-----
This system is the Elected BSR
BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
Next bootstrap message in 00:01:00
Configuration:
  Candidate loopback 2 (Address 1.51.51.1). Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisement in 00:01:00
RP: 1.51.51.1
  group prefixes:
    224.0.0.0 / 4
Candidate-RP-advertisement period: 60
```

The following example shows information for a device that is not the BSR.

```
device(config)# show ip pim bsr
PIMv2 Bootstrap information
-----
BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisement in 00:00:30
RP: 1.51.51.3
  group prefixes:
    224.0.0.0 / 4
Candidate-RP-advertisement period: 60
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip pim mcache

Displays the multicast cache.

## Syntax

```
show ip pim mcache [ A.B.C.D | ecmp ipv4 address ]
```

## Parameters

*A.B.C.D*

Specifies the multicast group or source IP address.

**ecmp***ipv4 address*

Specifies the PIM ECMP IPv4 information.

## Modes

Privileged EXEC mode

## Usage Guidelines

## Examples

The following example displays the output for **show ip pim mcache ip-address-1 ip-address-2**.

```
device# show ip pim mcache 50.1.1.101 230.1.1.1
IP Multicast Mcache Table
Entry Flags      : sm - Sparse Mode, ssm - Source Specific Multicast
                  RPT - RPT Bit, SPT - SPT Bit, LSrc - Local Source
                  LRcv - Local Receiver, RegProbe - Register In Progress
                  RegSupp - Register Suppression Timer, Reg - Register Complete
                  needRte - Route Required for Src/RP
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
                  MJ - Membership Join, BR - Blocked RPT, BA - Blocked Assert
                  BF - Blocked Filter
Total entries in mcache: 8
1 (50.1.1.101, 230.1.1.1) in Ve 40, Uptime 00:03:29
  Sparse Mode, RPT=0 SPT=1 Reg=0 RegSupp=0 RegProbe=0 LSrc=0 LRcv=1
  upstream neighbor=40.1.1.3
  num_oifs = 2
    Ve 2(00:03:29/181) Flags: IM
    Ve 10(00:03:29/0) Flags: MJ
Flags (0x400784d1)
  sm=1 ssm=0 needRte=0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip pim neighbor

Displays information about PIM neighbors.

## Syntax

```
show ip pim neighbor [ interface ethernet slot/port | interface ve ve-num ]
```

## Parameters

**interface ethernet** *slot/port*

Displays information for the specified Ethernet interface.

**interface ve** *ve-num*

Displays information for the specified VE interface.

## Modes

User EXEC mode

## Command Output

The **show ip pim neighbor** command displays the following information:

Output Field	Description
Port	The interface through which the device is connected to the neighbor.
Phyport	When there is a virtual interface, this is the physical port to which the neighbor is connected.
Neighbor	The IP interface of the PIM neighbor.
Holdtime sec	Indicates how many seconds the neighbor wants this device to hold the entry for this neighbor in memory. The neighbor sends the Hold Time in Hello packets: <ul style="list-style-type: none"> <li>If the device receives a new Hello packet before the Hold Time received in the previous packet expires, the device updates its table entry for the neighbor.</li> <li>If the device does not receive a new Hello packet from the neighbor before the Hold time expires, the device assumes the neighbor is no longer available and removes the entry for the neighbor.</li> </ul>
Age sec	The number of seconds since the device received the last hello message from the neighbor.
UpTime sec	The number of seconds the PIM neighbor has been up. This timer starts when the device receives the first Hello messages from the neighbor.
VRF	The VRF in which the interface is configured. This can be a VRF that the port was assigned to or the default VRF of the device.
Priority	The DR priority that is used in the DR election process. This can be a configured value or the default value of 1.

## Examples

The following example shows information about PIM neighbors.

```
device(config)# show ip pim neighbor
```

Port	PhyPort	Neighbor	Holdtime	T	PropDelay	Override	Age	UpTime	VRF	Prio
			sec	Bit	msec	msec	sec			
v2	e1/1	2.1.1.2	105	1	500	3000	0	00:44:10	default-vrf	1
v4	e1/2	4.1.1.2	105	1	500	3000	10	00:42:50	default-vrf	1
v5	e1/1	5.1.1.2	105	1	500	3000	0	00:44:00	default-vrf	1
v22	e1/1	22.1.1.1	105	1	500	3000	0	00:44:10	default-vrf	1

Total Number of Neighbors : 4

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ip pim rp-candidate

Displays candidate rendezvous point (RP) information.

## Syntax

```
show ip pim rp-candidate
```

## Parameters

**rp-candidate**

Specifies the candidate rendezvous point.

## Modes

User EXEC mode

## Usage Guidelines

When used without the **vrf** option, this command displays information for the default VRF.

## Command Output

The **show ip pim rp-candidate** command displays the following information:

Output Field	Description
Candidate-RP-advertisement in	How time will pass before the BSR sends the next RP message. The time is displayed in "hh:mm:ss" format.  <b>NOTE</b> This field appears only if this device is a candidate RP.
RP	The IP address of the RP.  <b>NOTE</b> This field appears only if this device is a candidate RP.
group prefixes	The multicast groups for which the RP listed by the previous field is a candidate RP.  <b>NOTE</b> This field appears only if this device is a candidate RP.
Candidate-RP-advertisement period	How frequently the BSR sends candidate RP advertisement messages.  <b>NOTE</b> This field appears only if this device is a candidate RP.

show ip pim rp-candidate

## Examples

The following example shows information for a candidate RP.

```
device> show ip pim rp-candidate
Next Candidate-RP-advertisement in 00:00:10
RP: 207.95.7.1
  group prefixes:
    224.0.0.0 / 4
Candidate-RP-advertisement period: 60
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip pim rp-hash

Displays rendezvous-point (RP) information for a PIM Sparse group.

## Syntax

```
show ip pim rp-hash group-addr
```

## Parameters

*group-addr*

Specifies the address of a PIM Sparse IP multicast group.

## Modes

Privileged EXEC mode

## Command Output

The **show ip pim rp-hash** command displays the following information:

Output Field	Description
RP	Indicates the IP address of the RP for the specified PIM Sparse group.
Info source	Indicates the source of the RP information. It can be a static-RP configuration or learned via the bootstrap router. If RP information is learned from the boot strap, the BSR IP address is also displayed.

## Examples

The following example shows RP information for a PIM Sparse group.

```
device# show ip pim rp-hash 239.255.162.1
RP: 207.95.7.1, v2
Info source: 207.95.7.1, via bootstrap
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip pim rp-map

Displays rendezvous-point (RP)-to-group mapping information.

## Syntax

```
show ip pim rp-map
```

## Modes

User EXEC mode

## Command Output

The **show ip pim rp-map** command displays the following information:

Output Field	Description
Group address	Indicates the PIM Sparse multicast group address using the listed RP.
RP address	Indicates the IP address of the RP for the listed PIM Sparse group.

## Examples

The following example shows RP-to-group mapping.

```
device> show ip pim rp-map
Number of group-to-RP mappings: 6
Group address      RP address
-----
1 239.255.163.1    99.99.99.5
2 239.255.163.2    99.99.99.5
3 239.255.163.3    99.99.99.5
4 239.255.162.1    99.99.99.5
5 239.255.162.2    43.43.43.1
6 239.255.162.3    99.99.99.5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip pim rp-set

Displays rendezvous-point (RP)-set list for the device elected as the bootstrap router (BSR).

## Syntax

```
show ip pim rp-set
```

## Modes

User EXEC mode

## Command Output

The **show ip pim rp-set** command displays the following information:

Output Field	Description
Number of group prefixes	The number of PIM Sparse group prefixes for which the RP is responsible.
Group prefix	Indicates the multicast groups for which the RP listed by the previous field is a candidate RP.
RPs expected or received	Indicates how many RPs were expected and received in the latest bootstrap message.
RP num	Indicates the RP number. If there are multiple RPs in the PIM Sparse domain, a line of information for each RP is listed, in ascending numerical order.
priority	The RP priority of the candidate RP. During the election process, the candidate RP with the highest priority is elected as the RP.
age	The age (in seconds) of this RP-set.
holdtime	Indicates the time in seconds for which this rp-set information is valid.  If this rp-set information is not received from BSR within the holdtime period, the rp-set information is aged out and deleted.

## Examples

The following example shows the RP set list for the device elected as BSR.

```
device> show ip pim rp-set
Static RP
-----
Static RP count: 2
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs: 2
  RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
  RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

The following example shows the RP set list for devices that are not elected as BSR.

```
device> show ip pim rp-set
Static RP
-----
Static RP count: 2
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs expected: 2
# RPs received: 2
  RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
  RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip pim rpf

Displays what PIM sees as the best reverse path to the source. While there may be multiple routes back to the source, the one displayed by this command is the one that PIM thinks is best.

## Syntax

```
show ip pim [ vrf vrf-name ] rpf A.B.C.D
```

## Parameters

**vrf** *vrf-name*

Displays information for the specified VRF instance.

*A.B.C.D*

Specifies the source address for reverse-path forwarding (RPF) check.

## Modes

User EXEC mode

## Examples

This example shows best reverse path to the specified source:

```
device# show ip pim vrf eng rpf 130.50.11.10
Source 130.50.11.10 directly connected on e1/1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip pim traffic

Displays IPv4 PIM traffic statistics.

## Syntax

```
show ip pim traffic
```

## Modes

Privileged EXEC mode

## Usage Guidelines

PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

## Command Output

The **show ip pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the PIM interface is configured.
HELLO	The number of PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface.  <b>NOTE</b> Unlike PIM Dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface.
Err	The total number of messages discarded, including a separate counter for those that failed the checksum comparison.



## Examples

This example shows PIM join and prune traffic statistics for received and sent packets:

```

device# show ip pim traffic
Port      |HELLO |JOIN  |PRUNE |ASSERT |GRAFT/REGISTER |REGISTER-STOP |BSR-MSGs |RPC-MSGs
          |Rx    |Rx    |Rx    |Rx     |Rx             |Rx           |Rx       |Rx
-----+-----+-----+-----+-----+-----+-----+-----+-----+
Ve10     | 54   | 0    | 0    | 0     | 0             | 0           | 0       | 0
Lo 1     | 0    | 0    | 0    | 0     | 0             | 0           | 0       | 0

device# show ip pim traffic
Port      |HELLO |JOIN  |PRUNE |ASSERT |GRAFT/REGISTER |REGISTER-STOP |BSR-MSGs |RPC-MSGs
          |Tx    |Tx    |Tx    |Tx     |Tx             |Tx           |Tx       |Tx
-----+-----+-----+-----+-----+-----+-----+-----+
Ve10     | 29   | 0    | 0    | 0     | 0             | 0           | 0       | 0
Lo 1     | 28   | 0    | 0    | 0     | 0             | 0           | 0       | 0

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ip route

Displays IP route information for IPv4 interfaces.

## Syntax

```
show ip route [ vrf vrf-name ]
show ip route A.B.C.D [ vrf vrf-name ]
show ip route A.B.C.D/M [ longer ] [ vrf vrf-name ]
show ip route all [ vrf vrf-name ]
show ip route bgp [ vrf vrf-name ]
show ip route connected [ vrf vrf-name ]
show ip route import [ src-vrf-name ] [ vrf vrf-name ]
show ip route isis
show ip route nexthop [ nexthopID [ ref-routes ] ] [ vrf vrf-name ]
show ip route ospf [ vrf vrf-name ]
show ip route slot line-card-number [ A.B.C.D | A.B.C.D/M ] [ vrf vrf-name ]
show ip route static [ vrf vrf-name ]
show ip route summary [ vrf vrf-name ]
show ip route system-summary
```

## Parameters

**vrf vrf-name**  
Specifies routes for a selected VRF instance.

**A.B.C.D/M**  
Specifies the IPv4 address and optional mask.

**longer**  
Specifies routes that match the specified prefix.

**all**  
Specifies information for all configured IPv4 routes.

**bgp**  
Specifies BGP route information.

**connected**  
Specifies directly connected routes, such as local Layer 3 interfaces.

**import**  
Specifies imported IPv4 routes.

**src-vrf-name**  
Specifies a VRF instance from which routes are leaked.

**isis**

Specifies routes under the Intermediate System to Intermediate System (IS-IS) protocol.

**nexthop**

Specifies the configured next hop.

*next-hop-ID*

Valid values range from 0 through 4294967294.

**ref-routes**

Specifies all routes that point to the specified *next-hop ID*.

**ospf**

Specifies routes learned from the Open Shortest Path First (OSPF) protocol.

**slot line-card-number**

Specifies routes with the provided line card number.

**static**

Specifies configured static routes.

**summary**

Specifies summary information for all routes.

**system-summary**

Specifies a system-level routing summary.

## Modes

Privileged EXEC mode

## Usage Guidelines

If leaked subnet routes are present, that information displays in the output.

To view the status of management routes, use the **show ip route vrf** command and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually. Example output is shown below.

```
device# show ip route vrf mgmt-vrf
IP Routing Table for VRF "mgmt-vrf"
Total number of IP routes: 3
 '*' denotes best ucast next-hop
 '[x/y]' denotes [preference/metric]

0.0.0.0/0
  *via 10.25.96.1, mgmt 1, [1/1], 8d15h, static, tag 0
10.25.96.0/22, attached
  *via DIRECT, mgmt 1, [0/0], 8d15h, direct, tag 0
10.25.96.38/32, attached
  *via DIRECT, mgmt 1, [0/0], 8d15h, local, tag 0
```

## Examples

The following example displays output for the **system-summary** option.

```
device# show ip route system-summary
System Route Count: 3 Max routes: 4096 (Route limit not exceeded)
System Nexthop Count: 2 Max nexthops: 1024 (Nexthop limit not exceeded)

VRF-Name: default-vrf
  Route count: 0 Max routes: Not Set (Route limit not exceeded)
  0 connected, 0 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS, 0 unnumbered

VRF-Name: mgmt-vrf
  Route count: 3 Max routes: Not Set (Route limit not exceeded)
  1 connected, 1 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS, 0 unnumbered
```

The following example displays output for the **connected** option.

```
device# show ip route connected
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
  Destination      Gateway           Port           Cost           Type Uptime
1      1.1.1.0/24      DIRECT           Te 2/1         0/0            D    4m33s
2      1.1.2.0/24      DIRECT           Te 2/2         0/0            D    2m42s
```

The following example displays output for the **summary** option.

```
device# show ip route summary
IP Routing Table - 7 entries:
  8 direct, 0 static, 0 RIP, 0 OSPF, 8 BGP, 0 ISIS, 80 EVPN Host
Number of prefixes:
  /24: 7
Nexthop Table Entry - 4 entries
```

The following example displays output for the **nexthop** option.

```
device# show ip route nexthop
Total number of IP nexthop entries: 4; Forwarding Use: 4
  NexthopIp      Port           RefCount      ID           Age
1      1.1.1.2      Te 2/1        3/3          2147549184 277
2      0.0.0.0      Te 2/2        1/1          2147484008 191
3      0.0.0.0      Te 2/1        2/2          2147484009 302
4      1.1.1.2      Te 2/1        1/1          2147549185 190
      1.1.2.2      Te 2/2
```

The following example displays output for a specific next-hop ID option.

```
device# show ip route nexthop 2147549184
  NexthopIp      Port           RefCount      ID           Age
1      1.1.1.2      Te 2/1        3/3          2147549184 288
```

The following example displays output for the **ref-routes** option.

```
device# show ip route nexthop 2147549184 ref-routes
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
  Destination      Gateway           Port           Cost           Type Uptime
1      100.1.1.0/24    1.1.1.2         Te 2/1         1/1            S    5m10s
2      100.1.2.0/24    1.1.1.2         Te 2/1         1/1            S    4m54s
3      100.1.3.0/24    1.1.1.2         Te 2/1         1
```

The following example displays output for a specific IP address.

```
device# show ip route 100.1.1.1
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
      Destination      Gateway      Port      Cost      Type  Uptime
4      100.1.1.0/24      1.1.1.2      Te 2/1      1/1      S      5m37s
```

The following example displays output for the **longer** option.

```
device# show ip route 100.0.0.0/8 longer
1      100.1.1.0/24      1.1.1.2      Te 2/1      1/1      S      14m37s
2      100.1.2.0/24      1.1.1.2      Te 2/1      1/1      S      14m21s
3      100.1.3.0/24      1.1.1.2      Te 2/1      1/1      S      14m18s
4      100.2.1.0/24      DIRECT      Te 2/1      1/1      S      14m2s
5      100.3.1.0/24      1.1.1.2      Te 2/1      1/1      S      13m10s
      100.3.1.0/24      1.1.2.2      Te 2/2      1/1      S      13m10s
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp

Displays BGP4+ route information.

## Syntax

```
show ipv6 bgp ipv6-addr [ /prefix ]
```

```
show ipv6 bgp { ipv6-addr [ /prefix ] } [ longer-prefixes | vrf vrf-name ]
```

## Parameters

*ipv6-addr*

IPv6 address of a neighbor in dotted-decimal notation, with optional mask.

*/prefix*

IPv6 mask length in CIDR notation.

**longer-prefixes**

Filters on prefixes equal to or greater than that specified by *prefix*.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays sample output from the **show ipv6 bgp** command.

```
device# show ipv6 bgp
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp attribute-entries

Displays BGP4+ route-attribute entries that are stored in device memory.

## Syntax

```
show ipv6 bgp attribute-entries [ vrf vrf-name ]
```

## Parameters

**vrf** *vrf-name*  
Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

The route-attribute entries table lists the sets of BGP4+ attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4+ route-attribute entries that are stored in device memory.

## Examples

This example show sample output for the **show ipv6 bgp attribute-entries** command.

```
device# show ipv6 bgp attribute-entries

Total number of BGP Attribute Entries: 1
1      Next Hop      : ::                                MED      :0          Origin:INCOMP
      Originator:0.0.0.0          Cluster List:None
      Aggregator:AS Number :0          Router-ID:0.0.0.0          Atomic:None
      Local Pref:100          Communities:Internet
      AS Path      : (length 0)
      AsPathLen: 0 AsNum: 0, SegmentNum: 0, Neighboring As: 0, Source As 0
      Address: 0x0b456c4c Hash:876 (0x03000000)
      Links: 0x00000000, 0x00000000
      Reference Counts: 1:0:1, Magic: 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp dampened-paths

Displays all BGP4+ dampened routes.

## Syntax

```
show ipv6 bgp dampened-paths [ vrf vrf-name ]
```

## Parameters

**vrf** *vrf-name*  
Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the **show ipv6 bgp dampened-paths** command.

```
device# show ipv6 bgp dampened-paths

      Status Code >:best d:damped h:history *:valid
      Network
Since  Reuse      Path                               From                               Flaps
*d 110:110:110:4::/64          160:160:160::10          36  0 :2 :
54  0 :10:10    111
*d 110:110:110:3::/64          160:160:160::10          36  0 :2 :
54  0 :10:10    111
*d 110:110:110:2::/64          160:160:160::10          36  0 :2 :
54  0 :10:10    111
*d 110:110:110:1::/64          160:160:160::10          36  0 :2 :
54  0 :10:10    111
*d 110:110:110::/64           160:160:160::10          36  0 :2 :
54  0 :10:10    111
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ipv6 bgp filtered-routes

Displays BGP4+ filtered routes that are received from a neighbor or peer group.

## Syntax

```
show ipv6 bgp filtered-routes [ detail ] [ ipv6-addr { / mask } [ longer-prefixes ] ] [ as-path-access-list name ] [ prefix-list name ] [ vrf vrf-name ]
```

## Parameters

### detail

Optionally displays detailed route information.

### ipv6-addr

IPv6 address of the destination network in dotted-decimal notation.

### mask

IPv6 mask of the destination network in CIDR notation.

### longer-prefixes

Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

### as-path-access-list name

Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

### prefix-list name

Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

### vrf vrf-name

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays BGP4+ filtered routes.

```
device# show ipv6 bgp filtered-routes
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp flap-statistics

Displays BGP4+ route-dampening statistics for all dampened routes with a variety of options.

## Syntax

```
show ipv6 bgp flap-statistics
```

```
show ipv6 bgp flap-statistics ipv6-addr { / mask } [ longer-prefixes [ vrf vrf-name ] | vrf vrf-name ]
```

```
show ipv6 bgp flap-statistics neighbor ipv6-addr [ vrf vrf-name ]
```

```
show ipv6 bgp flap-statistics regular-expression name [ vrf vrf-name ]
```

```
show ipv6 bgp flap-statistics vrf vrf-name
```

## Parameters

*ipv6-addr*

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

*mask*

IPv6 mask of a specified route in CIDR notation.

**longer-prefixes**

Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

**vrf** *vrf-name*

Specifies a VRF instance.

**neighbor**

Displays flap statistics only for routes learned from the specified neighbor.

*ip-addr*

IPv6 address of the neighbor.

**regular-expression**

Specifies a regular expression in the display output on which to filter.

*name*

Name of an AS-path filter or regular expression.

## Modes

Privileged EXEC mode

## Examples

This example displays flap statistics for a neighbor.

```
device# show ipv6 bgp flap-statistics neighbor 2001:
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors

Displays configuration information and statistics for BGP4+ neighbors of the device.

## Syntax

```
show ipv6 bgp neighbors [ ipv6-addr ]  
show ipv6 bgp neighbors last-packet-with-error [ vrf vrf-name ]  
show ipv6 bgp neighbors routes-summary [ vrf vrf-name ]  
show ipv6 bgp neighbors vrf vrf-name
```

## Parameters

*ipv6-addr*

IPv6 address of a neighbor in dotted-decimal notation.

**last-packet-with-error**

Displays the last packet with an error.

**route-summary**

Displays routes received, routes accepted, number of routes advertised by peer, and so on.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to view configuration information and statistics for BGP4+ neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

## Examples

This example shows sample output from the show ipv6 bgp neighbors command.

```
device# show ipv6 bgp neighbors

Total number of BGP Neighbors: 1
1  IP Address: 1:2::3, AS: 100 (IBGP), RouterID: 0.0.0.0, VRF: default-vrf
   State: CONNECT, Time: 0h3m3s, 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: 3
     Last update time was 172 sec ago
   Error: TCP status not available
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors advertised-routes

Displays the routes that the device has advertised to the neighbor during the current BGP4+ session.

## Syntax

```
show ipv6 bgp neighbors ipv6-addr advertised-routes [ detail | / mask-bits ] [ vrf vrf-name ]
```

## Parameters

*ipv6-addr*

IPv6 address of a neighbor in dotted-decimal notation.

**detail**

Displays details of advertised routes.

*mask-bits*

Number of mask bits in CIDR notation.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays the details of advertised routes.

```
device# show ipv6 bgp neighbors 123::3 advertised-routes

      There are 5 routes advertised to neighbor 123::3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
Prefix      Next Hop      MED      LocPrf      Weight      Status
1  110:110:110::/64  123::2      0          0          0          BE
   AS_PATH: 222 111
2  110:110:110:1::/64 123::2      0          0          0          BE
   AS_PATH: 222 111
3  110:110:110:2::/64 123::2      0          0          0          BE
   AS_PATH: 222 111
4  110:110:110:3::/64 123::2      0          0          0          BE
   AS_PATH: 222 111
5  110:110:110:4::/64 123::2      0          0          0          BE
   AS_PATH: 222 111
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors flap-statistics

Displays the route flap statistics for routes received from or sent to a BGP4+ neighbor.

## Syntax

```
show ipv6 bgp neighbors ipv6-addr flap-statistics [ vrf vrf-name ]
```

## Parameters

*ipv6-addr*

IPv6 address of a neighbor in dotted-decimal notation.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example shows flap statistics.

```
device#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors last-packet-with-error

Displays information about the last packet that contained an error from any of a device's neighbors.

## Syntax

```
show ipv6 bgp neighbors ipv6-addr last-packet-with-error [ decode ] [ vrf vrf-name ]
```

## Parameters

*ipv6-addr*

IPv6 address of a neighbor in dotted-decimal notation.

**decode**

Decodes last packet that contained an error from any of a device's neighbors.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode



## Examples

This example shows sample output from the **show ipv6 bgp neighbors last-packet-with-error** command when no packet from a specified neighbor contained an error.

```
device# show ipv6 bgp neighbors 123::3 last-packet-with-error

Received Message Length: 45
BGP Message:
 0xffffffff 0xffffffff 0xffffffff 0xffffffff 0x002d0104
 0x014b00b4 0x09090909 0x10020601 0x04020000 0x01020202
 0x00020280 0x00

BGP Header
Marker: 0xffffffff 0xffffffff 0xffffffff 0xffffffff
Message Length: (0x002d) 45
Message Type: (0x01) OPEN

OPEN Message
Version: (0x04) 4
AS Number: (0x014b) 331
Hold Time: (0x00b4) 180
BGP Identifier: (0x09090909) 9.9.9.9
Optional Parameter length: (0x10) 16

OPEN message optional parameters
Parameter Type: (0x02) Capability
Parameter Length: (0x06) 6
  Capability Type: (0x01) MULTIPROTOCOL EXTENSIONS
  Capability Length: (0x04) 4
  AFI: (0x0200) Unknown(512)
  Reserved: (0x00) 0
  SAFI: (0x01) Unicast

Parameter Type: (0x02) Capability
Parameter Length: (0x02) 2
  Capability Type: (0x02) ROUTE REFRESH(new)
  Capability Length: (0x00) 0

Parameter Type: (0x02) Capability
Parameter Length: (0x02) 2
  Capability Type: (0x80) ROUTE REFRESH(old)
  Capability Length: (0x00) 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4+ neighbors of the device.

## Syntax

**show ipv6 bgp neighbors** *ipv6-addr* **received**

**show ipv6 bgp neighbors** *ipv6-addr* **received detail** [ **vrf** *vrf-name* ]

**show ipv6 bgp neighbors** *ipv6-addr* **received prefix-filter** [ **vrf** *vrf-name* ]

**show ipv6 bgp neighbors** *ipv6-addr* **vrf** *vrf-name* ]

## Parameters

*ipv6-addr*

IPv6 address of a neighbor in dotted-decimal notation.

**detail**

Displays detailed information for ORFs received from BGP4+ neighbors of the device.

**vrf** *vrf-name*

Specifies a VRF instance.

**prefix-filter**

Displays the results for ORFs that are prefix-based.

## Modes

Privileged EXEC mode

## Examples

This example displays .

```
device# show ipv6 bgp neighbors 2001:db8:93e8:cc00::1 received prefix-filter
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors received-routes

Lists all route information received in route updates from BGP4+ neighbors of the device since the soft-reconfiguration feature was enabled.

## Syntax

```
show ipv6 bgp neighbors ipv6-addr received-routes [ detail ] [ vrf vrf-name ]
```

## Parameters

*ipv6-addr*

IPv4 address of a neighbor in dotted-decimal notation.

**detail**

Displays detailed route information.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays the .

```
device# show ipv6 bgp neighbors 160:160:160::10 received-routes

      There are 5 received routes from neighbor 160:160:160::10
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
      E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
      S:SUPPRESSED F:FILTERED s:STALE
      Prefix          Next Hop          MED           LocPrf        Weight  Status
  1    110:110:110::/64  160:160:160::10  0              100           0       BE
      AS_PATH: 111
  2    110:110:110:1::/64 160:160:160::10  0              100           0       BE
      AS_PATH: 111
  3    110:110:110:2::/64 160:160:160::10  0              100           0       BE
      AS_PATH: 111
  4    110:110:110:3::/64 160:160:160::10  0              100           0       BE
      AS_PATH: 111
  5    110:110:110:4::/64 160:160:160::10  0              100           0       BE
      AS_PATH: 111
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors rib-out-routes

Displays information about BGP4+ outbound RIB routes.

## Syntax

```
show ipv6 bgp neighbors ipv6-addr rib-out-routes ipv6-addr mask [ vrf vrf-name ]
show ipv6 bgp neighbors ipv6-addr rib-out-routes detail ipv6-addr mask [ vrf vrf-name ]
show ipv6 bgp neighbors ipv6-addr rib-out-routes detail [ vrf vrf-name ]
show ipv6 bgp neighbors ipv6-addr rib-out-routes [ vrf vrf-name ]
```

## Parameters

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

*vrf vrf-name*  
Specifies a VRF instance.

**detail**  
Displays detailed RIB route information.

## Modes

Privileged EXEC mode

## Examples

This example shows sample output from the **show ipv6 bgp neighbors rib-out-routes** command.

```
device# show ipv6 bgp neighbors 123::3 rib-out-routes

      There are 5 RIB_out routes for neighbor 123::3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
Prefix      Next Hop      MED      LocPrf      Weight      Status
1    110:110:110::/64  160:160:160::10  0           100          0          BE
   AS_PATH: 111
2    110:110:110:1::/64 160:160:160::10  0           100          0          BE
   AS_PATH: 111
3    110:110:110:2::/64 160:160:160::10  0           100          0          BE
   AS_PATH: 111
4    110:110:110:3::/64 160:160:160::10  0           100          0          BE
   AS_PATH: 111
5    110:110:110:4::/64 160:160:160::10  0           100          0          BE
   AS_PATH: 111
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4+ neighbors.

## Syntax

```
show ipv6 bgp neighbors ipv6-addr routes [ best | not-installed-best | unreachable [ vrf vrf-name ] ]
show ipv6 bgp neighbors ipv6-addr routes detail [ best | not-installed-best | unreachable [ vrf vrf-name ] ]
show ipv6 bgp neighbors ipv6-addr routes detail [ vrf vrf-name ]
show ipv6 bgp neighbors ipv6-addr routes [ vrf vrf-name ]
```

## Parameters

*ipv6-addr*

IPv6 address of a neighbor in dotted-decimal notation.

**best**

Displays routes received from the neighbor that are the best BGP4+ routes to their destination.

**not-installed-best**

Displays routes received from the neighbor that are the best BGP4+ routes to their destination but were not installed in the route table because the device received better routes from other sources.

**unreachable**

Displays routes that are unreachable because the device does not have a valid OSPF or static route to the next hop.

**vrf *vrf-name***

Specifies a VRF instance.

**detail**

Displays detailed information for the specified route types.

## Modes

Privileged EXEC mode

## Examples

This example shows sample output from the **show ipv6 bgp neighbors routes** command when the **best** keyword is used.

```
device# show ipv6 bgp neighbor 2001:db8::106 routes best
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4+ neighbors.

## Syntax

```
show ipv6 bgp neighbors ipv6-addr routes-summary [ vrf vrf-name ]
```

## Parameters

*ipv6-addr*

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

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Command Output

The **show ipv6 bgp neighbors routes-summary** command displays the following information.

Output field	Description
IP Address	The IPv6 address of the neighbor
Routes Received	How many routes the device has received from the neighbor during the current BGP4+ session: <ul style="list-style-type: none"> <li>Accepted or Installed - Indicates how many of the received routes the device accepted and installed in the BGP4+ route table.</li> <li>Filtered or Kept - Indicates how many routes were filtered out, but were nonetheless retained in memory for use by the soft reconfiguration feature.</li> <li>Filtered - Indicates how many of the received routes were filtered out.</li> </ul>
Routes Selected as BEST Routes	The number of routes that the device selected as the best routes to their destinations.
BEST Routes not Installed in IPv6 Forwarding Table	The number of routes received from the neighbor that are the best BGP4+ routes to their destinations, but were nonetheless not installed in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, or static IPv6 routes).
Unreachable Routes	The number of routes received from the neighbor that are unreachable because the device does not have a valid OSPFv3, or static IPv6 route to the next hop.
History Routes	The number of routes that are down but are being retained for route flap dampening purposes.

Output field	Description
NLRIs Received in Update Message	The number of routes received in Network Layer Reachability (NLRI) format in UPDATE messages: <ul style="list-style-type: none"> <li>Withdraws - The number of withdrawn routes the device has received.</li> <li>Replacements - The number of replacement routes the device has received.</li> </ul>
NLRIs Discarded due to	Indicates the number of times the device discarded an NLRI for the neighbor due to the following reasons: <ul style="list-style-type: none"> <li>Maximum Prefix Limit - The device's configured maximum prefix amount had been reached.</li> <li>AS Loop - An AS loop occurred. An AS loop occurs when the BGP4+ AS-path attribute contains the local AS number.</li> <li>Invalid Nexthop Address - The next hop value was not acceptable.</li> <li>Duplicated Originator_ID - The originator ID was the same as the local router ID.</li> <li>Cluster_ID - The cluster list contained the local cluster ID, or contained the local router ID (see above) if the cluster ID is not configured.</li> </ul>
Routes Advertised	The number of routes the device has advertised to this neighbor: <ul style="list-style-type: none"> <li>To be Sent - The number of routes the device has queued to send to this neighbor.</li> <li>To be Withdrawn - The number of NLRIs for withdrawing routes the device has queued up to send to this neighbor in UPDATE messages.</li> </ul>
NLRIs Sent in Update Message	The number of NLRIs for new routes the device has sent to this neighbor in UPDATE messages: <ul style="list-style-type: none"> <li>Withdraws - The number of routes the device has sent to the neighbor to withdraw.</li> <li>Replacements - The number of routes the device has sent to the neighbor to replace routes the neighbor already has.</li> </ul>
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: <ul style="list-style-type: none"> <li>Receiving Update Messages - The number of times UPDATE messages were discarded because there was no memory for attribute entries.</li> <li>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.</li> <li>Attributes - The number of times there was no memory for BGP4+ attribute entries.</li> <li>Outbound Routes (RIB-out) - The number of times there was no memory to place a "best" route into the neighbor's route information base (Adj-RIB-Out) for routes to be advertised.</li> <li>Outbound Routes Holder - For debugging purposes only.</li> </ul>

show ipv6 bgp neighbors routes-summary

## Examples

This example shows sample output from the **show ipv6 bgp neighbors routes-summary** command.

```
device# show ipv6 bgp neighbors routes-summary
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ipv6 bgp peer-group

Displays peer-group information.

## Syntax

```
show ipv6 bgp peer-group peer-group-name [ vrf vrf-name ]
```

## Parameters

*peer-group-name*

Specifies a peer group name.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Only the parameters that have values different from their defaults are listed.

## Examples

This example shows sample output from the **show ipv6 bgp peer-group** command.

```
device# show ipv6 bgp peer-group

1  BGP peer-group is pg
   Address family : IPV4 Unicast
   activate
   Address family : IPV6 Unicast
   no activate
   Members:
   IP Address: 1.1.1.1, AS: 100
   IP Address: 1::1, AS: 100

2  BGP peer-group is pg6
   Address family : IPV4 Unicast
   activate
   Address family : IPV6 Unicast
   no activate
   Currently there are no members.
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp routes

Displays BGP4+ route information that is filtered by the table entry at which the display starts.

## Syntax

```
show ipv6 bgp routes [ num | ipv6-address/prefix | age num | as-path-access-list name | best | cidr-only | community-access-list name | community-reg-expression expression | detail | local | neighbor ipv6-addr | nexthop ipv6-addr | no-best | not-installed-best | prefix-list string | regular-expression name | route-map name | summary | unreachable ] [ vrf vrf-name ]
```

## Parameters

*num*

Table entry at which the display starts.

*ipv6-address/prefix*

Table entry at which the display starts.

**age**

Displays BGP4+ route information that is filtered by age.

**as-path-access-list** *name*

Displays BGP4+ route information that is filtered by autonomous system (AS)-path access control list (ACL). The name must be between 1 and 32 ASCII characters in length.

**best**

Displays BGP4+ route information that the device selected as best routes.

**cidr-only**

Displays BGP4+ routes whose network masks do not match their class network length.

**community-access-list** *name*

Displays BGP4+ route information for an AS-path community access list. The name must be between 1 and 32 ASCII characters in length.

**community-reg-expression** *expression*

Displays BGP4+ route information for an ordered community-list regular expression.

**detail**

Displays BGP4+ detailed route information.

**local**

Displays BGP4+ route information about selected local routes.

**neighbor** *ip-addr*

Displays BGP4+ route information about selected BGP neighbors.

**nexthop** *ip-addr*

Displays BGP4+ route information about routes that are received from the specified next hop.

**no-best**

Displays BGP4+ route information that the device selected as not best routes.

**not-installed-best**

Displays BGP4+ route information about best routes that are not installed.

**prefix-list** *string*

Displays BGP4+ route information that is filtered by prefix list. The string must be between 1 and 32 ASCII characters in length.

**regular-expression** *name*

Displays BGP4+ route information about routes that are associated with the specified regular expression.

**route-map** *name*

Displays BGP4+ route information about routes that use the specified route map.

**summary**

Displays BGP4+ summary route information.

**unreachable**

Displays BGP4+ route information about routes whose destinations are unreachable through any of the BGP4+ paths in the BGP4+ route table.

**vrf** *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example shows sample input from the **show ipv6 bgp routes** command.

```
device# show ipv6 bgp routes

Total number of BGP Routes: 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
S:SUPPRESSED F:FILTERED s:STALE
Prefix           Next Hop           MED           LocPrf         Weight Status
1                107:1:1::/64      ::            0              100          32768 BL
AS_PATH:
```

This example shows sample input from the **show ip bgp routes** command when the **summary** keyword is used.

```
device# show ipv6 bgp routes summary

Total number of BGP routes (NLRIs) Installed      : 1
Distinct BGP destination networks                 : 1
Filtered bgp routes for soft reconfig             : 0
Routes originated by this router                  : 1
Routes selected as BEST routes                    : 1
Routes Installed as BEST routes                   : 1
BEST routes not installed in IP forwarding table  : 0
Unreachable routes (no IGP route for NEXTHOP)    : 0
IBGP routes selected as best routes               : 0
EBGP routes selected as best routes               : 0
BEST routes not valid for IP forwarding table     : 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp routes community

Displays BGP4+ route information that is filtered by community and other options.

## Syntax

```
show ipv6 bgp routes community { num | internet | local-as | no-advertise | no-export } [ vrf vrf-name ]
```

## Parameters

### community

Displays routes filtered by a variety of communities.

### *num*

Specific community member.

### internet

Displays routes for the Internet community.

### local-as

Displays routes for a local sub-AS within the confederation.

### no-advertise

Displays routes with this community that cannot be advertised to any other BGP4+ devices at all.

### no-export

Displays routes for the community of sub-ASs within a confederation.

### vrf *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows output from the **show ipv6 bgp routes community** command when the **internet** keyword is used.

```
device# show ipv6 bgp routes community internet
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 bgp summary

Displays BGP information such as the local autonomous system number (ASN), maximum number of routes supported, and some BGP4+ statistics.

## Syntax

```
show ipv6 bgp summary [ vrf vrf-name ]
```

## Parameters

**vrf vrf-name**  
Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

This example displays summary BGP4+ information.

```
device# show ipv6 bgp summary

BGP4 Summary
Router ID: 107.1.1.8   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: 1, Uses 96 bytes
Number of Routes Advertising to All Neighbors: 1 (1 entries), Uses 60 bytes
Number of Attribute Entries Installed: 1, Uses 104 bytes
Neighbor Address  AS#      State   Time    Rt:Accepted  Filtered  Sent    ToSend
1:2::3           100     CONN   0h 0m18s  0           0         0       1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 counters interface

Displays ipv6 statistics for an interface.

## Syntax

```
show ipv6 counters interface [ ethernet slot/port | loopback loopback-number | ve ve-number ]
```

## Parameters

### interface

Specifies an interface.

### ethernet *slot/port*

Specifies physical Ethernet interface and a valid slot and port on it.

### loopback *loopback-number*

Specifies the loopback interface.

### ve *ve-number*

Specifies the virtual Ethernet (ve) number.

## Modes

Privileged EXEC mode

## Examples

The following is an example of the **show ipv6 counters interface** command output.

```
device# show ipv6 counters interface ethernet 1/1
Interface Ethernet 1/1 IPv6 statistics (ifindex 406896641)
```

## History

Release version	Command history
16.1.00	This command was introduced.

# show ipv6 dhcp relay address interface

Displays IPv6 DHCP Relay addresses configured on supported interfaces.

## Syntax

```
show ipv6 dhcp relay address interface [ ethernet slot/port | ve interface number ]
```

## Parameters

### ethernet

Specifies the ethernet interface.

### slot

Specifies a valid slot number.

### port

Specifies a valid port number.

### ve

Specifies the Ve interface.

### interface number

Specifies the Ve interface number.

## Modes

Privileged EXEC mode

## Examples

The following example displays IPv6 DHCP relay address(es) configured per interface.

```
device# show ipv6 dhcp relay address interface ethernet 3/21
```

Interface	Relay Address	VRF Name	Outgoing Interface
Eth 3/21	4001::101	default-vrf	
Eth 3/21	fe80::8	blue	Ve 100

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ipv6 dhcp relay statistics

Displays general information about the DHCPv6 Relay function.

## Syntax

```
show ipv6 dhcp relay statistics
```

## Modes

Privileged EXEC mode

## Usage Guidelines

The **show ipv6 dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on the device:

- Number of DHCP Error packets dropped.
- Number of DHCP SOLICIT, REQUEST, CONFIRM, RENEW, REBIND, RELEASE, DECLINE, INFORMATION-REQUEST, RELAY-FORWARD, RELAY-REPLY packets received.
- Number of DHCP RELAY-FORWARD, REPLY packets sent.

## Examples

To display statistics for the device:

```
device# show ipv6 dhcp relay statistics

Packets dropped          : 0
  Error                  : 0
Packets received        : 0
  SOLICIT                : 0
  REQUEST                : 0
  CONFIRM                : 0
  RENEW                  : 0
  REBIND                 : 0
  RELEASE                : 0
  DECLINE                : 0
  INFORMATION-REQUEST    : 0
  RELAY-FORWARD          : 0
  RELAY-REPLY            : 0
Packets sent            : 0
  RELAY-FORWARD          : 0
  REPLY                  : 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 interface

Displays details of IPv6 interfaces.

## Syntax

```
show ipv6 interface [ brief | ethernet slot/port | loopback loopback-port-number | ve ve_id ]
```

## Parameters

### brief

Displays brief interface information.

### ethernet

Specifies Ethernet interface.

#### *slot*

Specifies a valid slot number.

#### *port*

Specifies a valid port number.

### loopback *loopback-port-number*

Specifies the loopback interface. The range is from 1 to 255.

### ve *ve-id*

Specifies the VE ID of a virtual Ethernet (VE) interface. The range is from 1 to 4096.

## Modes

Privileged EXEC mode

Interface configuration mode

## Examples

The following example displays the output of the **show ipv6 interface** command with an Ethernet interface specified:

```
device# show ipv6 interface ethernet 2/25
Ethernet 2/25 is up protocol is up
IPv6 Address: 2025:2525:aaaa::1/64 Primary Confirmed
IPv6 Address: 2500:ffee:1234::12/64 Secondary Confirmed
IPv6 Address: 2500:ffee:1234::14/64 Secondary Confirmed
IPv6 Address: 2500:ffee:1234::16/64 Secondary Confirmed
IPv6 Address: fe80::748e:f8ff:fe09:e10d/128 Link-local Confirmed
IPv6 multicast groups locally joined:
  ff02::1
  ff02::2    ff02::1:ff00:1    ff02::1:ff00:12
  ff02::1:ff00:14    ff02::1:ff00:16    ff02::1:ff09:e10d

IPv6 MTU: 1500
Vrf : default-vrf
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 nd

Displays the router advertisement information.

## Syntax

```
show ipv6 nd interface [ ethernet slot/port | prefix | ve ve-number | vrf vrf-name ]
```

## Parameters

### interface

Specifies an interface.

### ethernet *slot/port*

Specifies physical Ethernet interface and a valid slot and port on it.

### prefix

Displays prefix information.

### ve *ve-number*

Specifies the virtual Ethernet (ve) number.

### vrf *vrf-name*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following is an example of the **show ipv6 nd** command output.

```
device# show ipv6 nd interface ethernet 3/5
ICMPv6 ND Interfaces for VRF default-vrf
IPv6 address: 2ffe::1
Router-Advertisement active timers:
  Last Router-Advertisement sent: 00:01:25
  Next Router-Advertisement sent in: 00:07:06
Router-Advertisement parameters:
  Periodic interval: 200 to 600 seconds
  Send 'Managed Address Configuration' flag: false
  Send 'Other Stateful Configuration' flag: false
  Send 'Current Hop Limit' field: 64
  Send 'MTU' option value: 1500
  Send 'Router Lifetime' field: 1800 secs
  Send 'Reachable Time' field: 0 ms
  Send 'Retrans Timer' field: 0 ms
  Suppress RA: false
  Suppress MTU in RA: false
  Suppress All RA: false
Neighbor-Solicitation parameters:
  NS retransmit interval: 1 secs
  DAD Attempts: 2
  DAD expiry: 1 secs
  Neighbor Cache Expiry: 14400 secs
```

## History

Release version	Command history
16.1.00	This command was introduced.

# show ipv6 neighbor

Displays the IPv6 neighbors.

## Syntax

```
show ipv6 neighbor [ ipv6-address | ethernet slot/port | static | dynamic | summary | ve ] vrf vrf-name
```

## Parameters

*ipv6-address*

Restricts the display to the entries for the specified IPv6 address. Specify this parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373.

**ethernet** *slot/port*

Restricts the display to the entries for the specified Ethernet interface.

**static**

Displays the static IPv6 neighbors.

**dynamic**

Displays the dynamic IPv6 neighbors .

**summary**

Displays the summary of IPv6 neighbors.

**ve** *ve-num*

Restricts the display to the entries for the specified VE interface. The range is from 1 to 4096.

**vrf** *vrf-name*

Displays the IPv6 neighbor information for the specified Virtual Routing/Forwarding (VRF) instance.

## Modes

User EXEC mode

## Examples

The following example displays the IPv6 neighbor table.

```
device# show ipv6 neighbor summary
No of Total Entries   No of Static Entries   No of Dynamic Entries
-----
2003                   0                       2003
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf

Displays OSPFv3 information.

## Syntax

```
show ipv6 ospf [ vrf name ]
```

## Parameters

*vrf name*

Specifies the name of the VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the show ipv6 ospf command.

```
device# show ipv6 ospf
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf area

Displays the OSPFv3 area table in a specified format.

## Syntax

```
show ipv6 ospf area [ A.B.C.D ] [ decimal ] [ vrf vrfname ]
```

## Parameters

*A.B.C.D*

Area address in dotted decimal format.

*decimal*

Area address in decimal format. Valid values range from 0 to 2147483647.

**vrf** *vrf name*

Specifies a non-default VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the **show ipv6 ospf area** command when no arguments or keywords are used.

```
device# show ipv6 ospf area
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ipv6 ospf database

Displays lists of information about different OSPFv3 link-state advertisements (LSAs).

## Syntax

```
show ipv6 ospf database [ advrtr A.B.C.D | extensive | grace | link-id decimal | prefix ipv6-addr ] [ vrf vrfname ]
show ipv6 ospf database [ as-external | inter-prefix | inter-router | intra-prefix | link [ decimal ] | network | router | type-7 ]
  [ advrtr A.B.C.D | link-id decimal ] [ vrf vrfname ]
show ipv6 ospf database scope { area { A.B.C.D | decimal } | as | link } [ vrf vrfname ]
show ipv6 ospf database summary [ all-vrfs | vrf vrfname ]
```

## Parameters

**advrtr** *A.B.C.D*

Displays LSAs by Advertising Router Id in dotted decimal format.

**extensive**

Displays detailed lists of LSA information.

**grace**

Displays grace LSA information.

**link-id** *decimal*

Link-state ID that differentiates LSAs. Valid values range from 1 through 4294967295.

**prefix**

Display LSAs that contain a prefix.

*ipv6-addr*

Specifies an IPv6 address.

**vrf vrf name**

Specifies a non-default VRF instance.

**as-external**

Displays information about external LSAs.

**inter-prefix**

Displays information about inter area prefix LSAs.

**inter-router**

Displays information about inter area router LSAs.

**intra-prefix**

Displays information about intra area prefix LSAs.

**link** *decimal*

Displays information about the link LSAs.

**network**

Displays information about network LSAs.

- router**  
Displays information about router LSAs.
- type-7**  
Displays information about the not so stubby area (NSSA) external LSAs.
- scope**  
Displays LSA information by LSA scope.
- area**  
Displays LSAs by scope within a specified area.
- as**  
Displays autonomous system (AS) LSAs by scope.
- link**  
Displays link LSAs by scope.
- summary**  
Displays LSA summary information.
- all-vrfs**  
Specifies all VRFs.

## Modes

Privileged EXEC mode

## Examples

The following is sample output from the **show ipv6 ospf database as-external** command using the **link-id** keyword:

```
device# show ipv6 ospf database as-external link-id 5
```

The following is sample output from the **show ipv6 ospf database inter-prefix** command using the **link-id** keyword:

```
device# show ipv6 ospf database inter-prefix link-id 5
```

The following is sample output from the **show ipv6 ospf database network** command:

```
device# show ipv6 ospf database network
```

The following is sample output from the **show ipv6 ospf database router** command:

```
device# show ipv6 ospf database router
```

The following is sample output from the **show ipv6 ospf database type-7** command:

```
device# show ipv6 ospf database type-7
```

The following is sample output from the **show ipv6 ospf database scope** command using the **area** keyword:

```
device# show ipv6 ospf database scope area 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf interface

Displays interface information for all or specific OSPFv3-enabled interfaces.

## Syntax

```
show ipv6 ospf interface brief [ all-vrfs | vrf vrf-name ]
```

```
show ipv6 ospf interface [ ethernet slot/port | loopback number | ve vlan_id ]
```

```
show ipv6 ospf interface [ vrf vrf-name ]
```

## Parameters

### brief

Displays summary information.

### all-vrfs

Displays the information for all VRF instances.

### vrf *vrf-name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

### ethernet *slot/port*

Specifies an Ethernet slot and port.

### loopback *number*

Specifies a loopback port number. Valid values range from 1 through 255.

### ve *vlan\_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

## Modes

Privileged EXEC mode

## Examples

The following is sample output from the **show ipv6 ospf interface** command when no arguments or keywords are used.

The following is sample output from the **show ipv6 ospf interface** command the **brief** keyword is used.

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf memory

Displays information about OSPFv3 memory usage.

## Syntax

```
show ipv6 ospf memory [ vrf vrfname ]
```

## Parameters

**vrf** *vrfname*

Displays the information for the specified VRF instance.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display routes that have been redistributed into OSPFv3.

## Examples

The following is sample output from the **show ipv6 ospf memory** command when no arguments or keywords are used:

```
device# show ipv6 ospf memory
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf neighbor

Displays detailed or summary OSPFv3 neighbor information.

## Syntax

```
show ipv6 ospf neighbor [ all-vrfs | vrf vrf-name ]
show ipv6 ospf neighbor detail [ vrf vrf-name ]
show ipv6 ospf neighbor interface [ ethernet slot/port | loopback number | ve vlan_id ]
show ipv6 ospf neighbor router-id A.B.C.D [ vrf vrf-name ]
```

## Parameters

### all-vrfs

Specifies all VRF instances.

### vrf *vrf-name*

Specifies a non-default VRF instance.

### detail

Specifies detailed neighbor information.

### interface

Displays OSPFv3 interface information.

### ethernet *slot/port*

Specifies an Ethernet slot and port.

### loopback *number*

Specifies a loopback port number. Valid values range from 1 through 255.

### ve *vlan\_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

### router-id *A.B.C.D*

Specifies neighbor information for the specified router ID (in dotted decimal format).

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the **show ipv6 ospf neighbor** command when no arguments or keywords are used.

```
device# show ipv6 ospf neighbor
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf redistribute route

Displays all IPv6 routes or a specified IPv6 route that the device has redistributed into OSPFv3.

## Syntax

```
show ipv6 ospf redistribute route A.B.C.D:M [ vrf vrf-name ]
```

```
show ipv6 ospf redistribute route [ vrf vrf-name ]
```

## Parameters

*A.B.C.D:M*

Specifies an IPv6 address.

**vrf** *vrfname*

Specifies the name of a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following is sample output from the **show ipv6 ospf redistribute route** command when no arguments or keywords are used:

```
device# show ipv6 ospf redistribute route
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show ipv6 ospf routes

Displays OSPFv3 routes.

## Syntax

```
show ipv6 ospf routes A.B.C.D:M [ vrf vrfname ]
```

```
show ipv6 ospf routes [ vrf vrfname ]
```

## Parameters

*A.B.C.D:M*

Specifies a destination IPv6 address.

vrf *vrfname*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example displays OSPFv3-calculated routes.

```
device# show ipv6 ospf routes
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf spf

Displays OSPFv3 SPF node, table, and tree information.

## Syntax

```
show ipv6 ospf spf { node | table | tree } [ area { A.B.C.D | decimal } ] [ vrf vrfname ]
```

## Parameters

### node

Displays OSPFv3 node information.

### table

Specifies a SPF table.

### tree

Specifies a SPF tree.

### area

Specifies an area.

*A.B.C.D*

Area address in dotted decimal format.

*decimal*

Area address in decimal format.

### vrf vrfname

Specifies a non-default VRF instance.

## Examples

The following example shows sample output from the **show ipv6 ospf spf** command when the **node** keyword is used.

```
device# show ipv6 ospf spf node
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf summary

Displays summary information for all OSPFv3 instances.

## Syntax

```
show ipv6 ospf summary [ all-vrfs | vrf vrfname ]
```

## Parameters

### **all-vrfs**

Specifies all VRF instances.

### **vrf *vrfname***

Specifies a non-default VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the **show ipv6 ospf summary** command when no arguments or keywords are used.

```
device# show ipv6 ospf summary
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf virtual-links

Displays information about all OSPFv3 virtual links or specified links.

## Syntax

```
show ipv6 ospf virtual-links brief [ vrf vrfname ]
```

```
show ipv6 ospf virtual-links [ vrf vrfname ]
```

## Parameters

**brief**

Displays summary information.

**vrf vrfname**

Specifies a non-default VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following is sample output from the **show ipv6 ospf virtual-links** command when no arguments or keywords are used:

```
device# show ipv6 ospf virtual-links
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 ospf virtual-neighbor

Displays information about OSPFv3 virtual neighbors.

## Syntax

```
show ipv6 ospf virtual-neighbor brief [ vrf vrfname ]
```

```
show ipv6 ospf virtual-neighbor [ vrf vrfname ]
```

## Parameters

**brief**

Displays summary information.

**vrf** *vrfname*

Specifies a nondefault VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following example shows sample output from the **show ipv6 ospf virtual-neighbor** command when no arguments or keywords are used.

```
device# show ipv6 ospf virtual-neighbor
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 prefix-list

Displays IPv6 prefix-lists.

## Syntax

```
show ipv6 prefix-list prefix-list-name
```

## Parameters

*prefix-list-name*

Specifies an IPv6 prefix list name.

## Modes

User EXEC mode

## Usage Guidelines

The *prefix-list-name* parameter restricts the display to the specified prefix list. Specify the name of the prefix list that you want to display.

## Command Output

The **show ipv6 prefix-list** command displays the following information:

## Examples

The following example shows how to display IPv6 prefix lists.

```
device# show ipv6 prefix-lists
ipv6 prefix-list routesfor2001: 2 entries
  seq 5 permit 2001::/16
  seq 10 permit 2001:db8::/32
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show ipv6 route

Displays the router advertisement information.

## Syntax

```
show ipv6 route [ all | bgp | connected | import source-name | nexthop nexthop-id | ospf | static | summary | system-  
summary ] vrf-name
```

```
show ipv6 route [ isis | slot linecard-number | static | system-summary | vrf number ]
```

## Parameters

**all**

Specifies all routes.

**bgp**

Specifies BGP routes.

**connected**

Displays the directly connected routes.

**import** *source-name*

Specifies import routes and the source VRF name

**isis**

Specifies ISIS routes.

**nexthop** *nexthop-id*

Displays the route nexthop table.

**ospf**

Specifies OSPF routes.

**slot** *linecard-number*

Specifies the IPv6 route information on a slot and the linecard number.

**static**

Specifies static IPv6 routes.

**summary**

Displays the route summary.

**system-summary**

Displays the system-level summary for IPv6 routes.

*vrf-name*

The name of the VRF context.

**vrf** *number*

Specifies a VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following is an example of the **show ipv6 route** command output.

```
SLX# show ipv6 route
IPv6 Routing Table for VRF "default-vrf"
Total number of IPv6 routes: 11
'*' denotes best ucast next-hop
'[x/y]' denotes [preference/metric]

1200:1201::/64, attached
  *via ::, Eth 2/45, [0/0], 45m29s, direct, tag 0
1200:1201::1:1/128, attached
  *via ::, Eth 2/45, [0/0], 45m29s, local, tag 0
1200:1202::/64, attached
  *via ::, Ve 2, [0/0], 45m26s, direct, tag 0
1200:1202::1:1/128, attached
  *via ::, Ve 2, [0/0], 45m26s, local, tag 0
2221::/32
  *via 1200:1201::1:2, Eth 2/45, [100/10], 11m41s, static, tag 300
2222::/48
  *via fe80::205:33ff:fee6:a531, Eth 2/45, [1/1], 43m44s, static, tag 0
2222::1/128
  *via fe80::205:33ff:fee6:a531, Eth 2/45, [110/1], 0m7s, ospfv3, intra, tag 0
2223::/64
  *via 1200:1202::1:2, Ve 2, [1/1], 3m45s, static, tag 0
2224::1/128
  *via fe80::205:33ff:fee6:a501, Ve 2, [1/1], 43m41s, static, tag 0
fe80::/10, attached
  *via ::, , [0/0], 6h30m, local, tag 0
ff00::/8, attached
  *via ::, Null0, [0/0], 6h30m, local, tag 0
```

## History

Release version	Command history
16.1.00	This command was introduced.



# show ipv6 static route

Displays information about IPv6 static routes.

## Syntax

```
show ipv6 static route [ ipv6prefix | vrf vrf-name ]
```

## Parameters

*ipv6prefix*

The IPv6 prefix in the *A:B::/length* format.

*vrf vrf-name*

The name of the VRF context.

## Modes

Privileged EXEC mode

## Examples

The following example displays the IPv6 static route information for the default VRF.

```
SLX# show ipv6 static route
IPv6 Configured Static Routes for VRF "default-vrf"

3002:7::/64-> 1200:3::1:2 preference: 1
  nh_vrf (default-vrf)

3002:9::/64-> 1200:4::1:2 preference: 1
  nh_vrf (default-vrf)
SLX#
```

# show ipv6 vrrp

Displays information about IPv6 VRRP and VRRP-E sessions.

## Syntax

```
show ipv6 vrrp
show ipv6 vrrp VRID [ detail | summary ]
show ipv6 vrrp detail
show ipv6 vrrp summary [ vrf { vrf-name | all | default-vrf } ]
show ipv6 vrrp interface [ ethernet slot/port ] [ detail | summary ]
show ipv6 vrrp interface ve vlan_id [ detail | summary ]
```

## Parameters

*VRID*

The virtual group ID about which to display information. The range is from 1 through 16.

**detail**

Displays all session information in detail, including session statistics.

**summary**

Displays session-information summaries.

**vrf**

Specifies a VRF instance or all VRFs.

*vrf-name*

Specifies a VRF instance. For the default vrf, enter **default-vrf**.

**all**

Specifies all VRFs.

**interface**

Displays information for an interface that you specify.

**ethernet** *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

**ve** *vlan\_id*

Specifies the VE VLAN number.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display information about IPv6 VRRP and VRRP-E sessions, either in summary or full-detail format. You can also specify a particular virtual group ID, or an interface for which to display VRRP output.

**NOTE**

IPv6 VRRP-E supports only the VE interface type.

To display information for IPv6 VRRP sessions using the default VRF, you can use the **show ipv6 vrrp summary** syntax (with no additional parameters).

To display information for the default or a named VRF, you can use the **show ipv6 vrrp summary vrf** syntax with the *vrf-name* option.

To display information about all VRFs, use the **show ipv6 vrrp summary vrf all** syntax.

## Examples

The following example displays information about all IPv6 VRRP sessions on the device.

```
device# show ipv6 vrrp

Total number of VRRP session(s)   : 2

VRID 14
  Interface: Ve 2018; Ifindex: 1207961570
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): fe80::1
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1000 milli sec (default: 1000 milli sec)
  Preempt mode: ENABLE (default: ENABLE)
  Hold time: 0 sec (default: 0 sec)
  Trackport:
    Port(s)                Priority  Port Status
    =====                =====  =====
  Statistics:
    Advertisements: Rx: 0, Tx: 35
    Neighbor Advertisements: Tx: 1

VRID 15
  Interface: Ve 2019; Ifindex: 1207961571
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): fe80::1
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1000 milli sec (default: 1000 milli sec)
  Preempt mode: ENABLE (default: ENABLE)
  Hold time: 0 sec (default: 0 sec)
  Trackport:
    Port(s)                Priority  Port Status
    =====                =====  =====
  Statistics:
    Advertisements: Rx: 0, Tx: 448
    Neighbor Advertisements: Tx: 1
```

The following example displays IPv6 VRRP information in detail for a specific virtual group ID of 19, including session statistics.

```

device# show ipv6 vrrp 19 detail

Total number of VRRP session(s)   : 1
VRID 15
  Interface: Ve 2019; Ifindex: 1207961571
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Backup
  Session Master IP Address: fe80::205:33ff:fe79:fb1e
  Virtual IP(s): 2001:2019:8192::1
  Virtual MAC Address: 02e0.5200.2513
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec (default: 1 sec)
  Preempt mode: DISABLE (default: DISABLED)
  Advertise-backup: ENABLE (default: DISABLED)
  Backup Advertisement interval: 60 sec (default: 60 sec)
  Short-path-forwarding: Enabled
  Revert-Priority: unset; SPF Reverted: No
  Hold time: 0 sec (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                Priority  Port Status
    =====                =====  =====
Global Statistics:
=====
Checksum Error : 0
Version Error  : 0
VRID Invalid   : 0
Session Statistics:
=====
Advertisements      : Rx: 103259, Tx: 1721
Neighbor Advertisements : Tx: 0
Session becoming master : 0
Advts with wrong interval : 0
Prio Zero pkts      : Rx: 0, Tx: 0
Invalid Pkts Rcvd   : 0
Bad Virtual-IP Pkts : 0
Invalid Authentication type : 0
Invalid TTL Value   : 0
Invalid Packet Length : 0
VRRPE backup advt sent : 1721
VRRPE backup advt recvd : 0

```

The following example displays summary information for IPv6 VRRP statistics on the default VRF. (This command is equivalent to **show ipv6 vrrp summary vrf default-vrf**.)

```

device# show ipv6 vrrp summary

Total number of VRRP session(s)   : 1
Master session count : 1
Backup session count  : 0
Init session count   : 0

VRID  Session  Interface  Admin  Current  State  Short-path  Revert  SPF
=====  =====  =====  =====  =====  =====  =====  =====  =====
15     VRRPE     Ve 2019   Enabled 100      Master  Enabled     unset   No

```

The following example displays summary information for IPv6 VRRP statistics on the VRF named red.

```
device# show ipv6 vrrp summary vrf red
```

```
Total number of VRRP session(s) : 1
Master session count : 1
Backup session count : 0
Init session count : 0
```

VRID	Session	Interface	Admin State	Current Priority	State	Short-path Forwarding	Revert Priority	SPF Reverted
14	VRRPE	Ve 2018	Enabled	100	Master	Enabled	unset	No

The following example displays summary information for IPv6 VRRP statistics on all VRFs.

```
device# show ipv6 vrrp summary vrf all
```

```
Total number of VRRP session(s) : 2
Master session count : 2
Backup session count : 0
Init session count : 0
```

VRID	Session	Interface	Admin State	Current Priority	State	Short-path Forwarding	Revert Priority	SPF Reverted
14	VRRPE	Ve 2018	Enabled	100	Master	Enabled	unset	No
15	VRRPE	Ve 2019	Enabled	100	Master	Enabled	unset	No

The following example displays information for IPv6 VRRP-E tracked networks.

```

device# show ipv6 vrrp detail

Total number of VRRP session(s)   : 1

VRID 2
Interface: Ve 100;  Ifindex: 1207959652
Mode: VRRPE
Admin Status: Enabled
Description :
Address family: IPv6
Version: 3
Authentication type: No Authentication
State: Master
Session Master IP Address: Local
Virtual IP(s): 2001:2019:8192::1
Virtual MAC Address: 02e0.5225.1002
Configured Priority: unset (default: 100); Current Priority: 100
Advertisement interval: 1 sec (default: 1 sec)
Preempt mode: DISABLE (default: DISABLED)
Advertise-backup: DISABLE (default: DISABLED)
Backup Advertisement interval: 60 sec (default: 60 sec)
Short-path-forwarding: Disabled
Revert-Priority: unset; SPF Reverted: No
Hold time: 0 sec (default: 0 sec)
Master Down interval: 4 sec
Trackport:
  Port(s)                Priority  Port Status
  =====                =====  =====

Tracknetwork:
  Network(s)             Priority  Status
  =====                =====  =====
  2001::/64              20      Up

Global Statistics:
=====
Checksum Error : 0
Version Error  : 0
VRID Invalid   : 0

Session Statistics:
=====
Advertisements           : Rx: 0, Tx: 132
Neighbor Advertisements  : Tx: 66
Session becoming master  : 1
Advts with wrong interval : 0
Prio Zero pkts           : Rx: 0, Tx: 0
Invalid Pkts Rvcd        : 0
Bad Virtual-IP Pkts      : 0
Invalid Authentication type : 0
Invalid TTL Value        : 0
Invalid Packet Length    : 0
VRRPE backup advt sent   : 0
VRRPE backup advt recvd  : 0

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis

Displays general IS-IS information.

## Syntax

**show isis**

## Modes

Privileged EXEC mode

## Command Output

The **show isis** command displays the following information:

Output field	Description
IS-IS Routing Protocol Operation State	The operating state of IS-IS. Possible states include the following: <ul style="list-style-type: none"> <li>• Enabled - IS-IS is enabled.</li> <li>• Disabled - IS-IS is disabled.</li> </ul>
IS-Type	The intermediate system type. Possible types include the following: <ul style="list-style-type: none"> <li>• Level 1 only - The device routes traffic only within the area in which it resides.</li> <li>• Level 2 only - The device routes traffic between areas of a routing domain.</li> <li>• Level 1-2 - The device routes traffic within the area in which it resides and between areas of a routing domain.</li> </ul>
System ID	The unique IS-IS router ID. Typically, the device's base MAC address is used as the system ID.
Manual area address(es)	Area address(es) of the device.
Level-1-2 Database State	The state of the Level 1-2 Database: <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> </ul>
Administrative Distance	The current setting of the IS-IS administrative distance.
Maximum Paths	The number of paths IS-IS can calculate and install in the forwarding table
Default redistribution metric	The value of the default redistribution metric, which is the IS-IS cost of redistributing the route into IS-IS.
Number of Routes redistributed into IS-IS	The number of routes distributed into IS-IS.
Level-1 Auth-mode	One of the following authentication modes set for Level-1 on the router: <ul style="list-style-type: none"> <li>• None</li> <li>• md5</li> <li>• cleartext</li> </ul>
Level-2 Auth-mode	One of the following authentication modes set for Level-2 on the router: <ul style="list-style-type: none"> <li>• None</li> <li>• md5</li> </ul>

Output field	Description
	<ul style="list-style-type: none"> <li>• cleartext</li> </ul>
Metric Style Supported for Level-1	<p>The following values are supported:</p> <ul style="list-style-type: none"> <li>• Wide - Wide Metric Style</li> <li>• Narrow - Narrow Metric Style</li> </ul>
Metric Style Supported for Level-2	<p>The following values are supported:</p> <ul style="list-style-type: none"> <li>• Wide - Wide Metric Style</li> <li>• Narrow - Narrow Metric Style</li> </ul>
IS-IS Partial SPF Optimizations	<p>This parameter can contain one of the following values:</p> <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Timers: L1 or L2 SPF:	These values are displayed individually for IS-IS levels 1 and 2.
max-wait	The maximum time gap that occurs between running of SPF calculations. It is the value configured as the <code>spf-max-wait</code> variable in the <code>spf-interval</code> command.
Init-wait	The initial time gap between an SPF event and the first running of SPF. This value reflects the <code>spf-initial-time</code> variable that is configured using the <code>spf-interval</code> command.
Second-wait	<p>The interval between the first running of SPF and the first recalculation of the SPF tree. If this optional value is configured, it is doubled with each recalculation of the SPF tree until the value is equal to the max-wait value</p> <p>This value reflects the <code>spf-second-wait</code> variable that is configured using the <code>spf-interval</code> command.</p>
SPF run status.	<p>This field is not specifically labeled but is displayed directly under the SPF timers. It can any of the three values shown below:</p> <ul style="list-style-type: none"> <li>• SPF is running</li> <li>• SPF will run in <code>sec</code> where the <code>sec</code> variable is a value in seconds until the next time that SPF will be run.</li> <li>• SPF is not scheduled</li> </ul>
Timers: PSPF:	
max-wait	The maximum time gap that occurs between running of PSPF calculations. It is the value configured as the <code>max-wait</code> value in the <code>partial-spf-interval</code> command.
Init-wait	The initial time gap between the wait time after an LSP change until the first PSPF calculation. This value reflects the <code>initial-wait</code> variable that is configured using the <code>partial-spf-interval</code> command.
Second-wait	<p>The wait time between the first and second PSPF calculations. If this optional value is configured, it is doubled with each PSPF recalculation until the value is equal to the max-wait value</p> <p>This value reflects the <code>second-wait</code> variable that is configured using the <code>partial-spf-interval</code> command.</p>
PSPF run status.	<p>This field is not specifically labeled but is displayed directly under the PSPF timers. It can any of the three values shown below:</p> <ul style="list-style-type: none"> <li>• PSPF is running</li> <li>• PSPF will run in <code>sec</code> where the <code>sec</code> variable is a value in seconds until the next time that PSPF will be run.</li> <li>• PSPF is not scheduled</li> </ul>
Timers: LSP:	



Output field	Description
max-lifetime	The maximum number of seconds an unrefreshed LSP can remain in the device's LSP database. The default value is 1000 sec.
refresh-interval	The maximum number of seconds that a device waits between sending updated LSPs to its IS-IS neighbors. The default value is 1 sec.
gen-interval	The minimum number of seconds that a device waits between sending updated LSPs to its IS-IS neighbors. The default value is 10 sec.
retransmit-interval	The amount of time the device waits before it retransmits LSPs. The default value is 5 sec.
lsp-interval	The rate of transmission (in milliseconds) of the LSPs. The default rate is 33 ms.
Timers: SNP:	
cstp-interval	How often the designated IS sends a CSNP to the broadcast interface. The default value is 10 sec.
psnp-interval	How often the IS sends a PSNP. The default value is 2 sec.
Global Hello Padding	This value can be: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Global Hello Padding For Point to Point Circuits	This value can be: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Ptpt Three Way HandShake Mechanism	This value can be: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
IS-IS Traffic Engineering Support	This value can be: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
BFD	This value can be: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Interfaces with IPv4 IS-IS configured	Interfaces on which IPv4 IS-IS is configured.

## Examples

This example displays sample output from the **show isis** command.

```
device# show isis

IS-IS Routing Protocol Operation State: Enabled
IS-Type: Level-1-2
System Id: 768e.f805.5812
Manual area address(es): 11
Level-1-2 Database State: On
Administrative Distance 115
Maximum Paths 8
Default redistribution metric 0
Default link metric for level-1 0 (conf)/ 10 (adv)
Default link metric for level-2 0 (conf)/ 10 (adv)
Protocol Routes Redistributed into IS-IS: None
Number of Routes Redistributed into IS-IS: 0
Level-1 Auth-mode: None
Level-2 Auth-mode: None
Metric Style Supported for Level-1: Narrow
Metric Style Supported for Level-2: Narrow
Graceful-Restart Helper Support: Enabled
ISIS Partial SPF Optimizations: Enabled
Timers:
  L1 SPF: Max-wait 5s Init-wait 5000ms Second-wait 5000ms
  L2 SPF: Max-wait 5s Init-wait 5000ms Second-wait 5000ms
    L1 SPF is not scheduled
    L2 SPF is not scheduled
  PSPF: Max-wait 5000ms Init-wait 2000ms Second-wait 5000ms
    PSPF is not scheduled
  LSP: max-lifetime 1200s refresh-interval 900s gen-interval 10s
    retransmit-interval 5s, lsp-interval 33ms
  SNP: csnp-interval 10s psnp-interval 2s
Global Hello Padding: Enabled
Global Hello Padding For Point to Point Circuits: Enabled
Ptpt Three Way HandShake Mechanism: Enabled
BGP Ipv4 Converged: False BGP Ipv6 Converged: False
IS-IS Traffic Engineering Support: Disabled
  No ISIS Shortcuts Configured
BFD: Disabled, BFD HoldoverInterval: 0
NSR: Disabled
LSP-SYNC: Not Globally Enabled
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis config

Displays the global IS-IS configuration commands that are in effect on the device.

## Syntax

```
show isis config
```

## Modes

Privileged EXEC mode

## Usage Guidelines

The running-config does not list the default values. Only commands that change a setting or add configuration information are displayed.

## Examples

This example displays sample output from the **show isis config** command.

```
device# show isis config

router isis
 net 11.768e.f805.5812.00
 address-family ipv4 unicast
 !

 address-family ipv6 unicast
 !
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis counts

Displays IS-IS error statistics.

## Syntax

**show isis counts**

## Modes

Privileged EXEC mode

## Command Output

The **show isis counts** command displays the following information:

Output field	Description
Area Mismatch	The number of times the device interface was unable to create a Level-1 adjacency with a neighbor because the device interface and the neighbor did not have any areas in common.
Max Area Mismatch	The number of times the device received a PDU whose value for maximum number of area addresses did not match the device's value for maximum number of area addresses.
System ID Length Mismatch	The number of times the device received a PDU whose ID field was a different length than the ID field length configured on the device.
LSP Sequence Number Skipped	The number of times the device received an LSP with a sequence number that was more than 1 higher than the sequence number of the previous LSP received from the same neighbor.
LSP Max Sequence Number Exceeded	The number of times the device attempted to set an LSP sequence number to a value higher than the highest number in the CSNP sent by the Designated IS.
Level-1 Database Overload	The number of times the Level-1 state on the device changed from Waiting to On or from On to Waiting. <ul style="list-style-type: none"> <li>Waiting to On - This change can occur when the device recovers from a previous Level-1 LSP database overload and is again ready to receive new LSPs.</li> <li>On to Waiting - This change can occur when the device's Level-1 LSP database is full and the device receives an additional LSP, for which there is no room.</li> </ul>
Level-2 Database Overload	The number of times the Level-2 state on the device changed from Waiting to On or from On to Waiting. <ul style="list-style-type: none"> <li>The change from Waiting to On can occur when the device recovers from a previous Level-2 LSP database overload and is again ready to receive new LSPs.</li> <li>The change from On to Waiting can occur when the device's Level-2 LSP database is full and the device receives an additional LSP, for which there is no room.</li> </ul>
Our LSP Purged	The number of times the device received an LSP that was originated by the device itself and had age zero (aged out).
PDU Drop Count	

Output field	Description
CSNP Auth Failures	The number of CSNP Authentication failures recorded for Level-1 and Level-2. This counter will only be displayed if it has a value greater than zero.
PSNP Auth Failures	The number of PSNP Authentication failures recorded for Level-1 and Level-2. This counter appears only if it has a value greater than 0.
HELLO Auth Failures	The number of HELLO Authentication failures recorded for Level-1 and Level-2. This counter will only be displayed if it has a value greater than zero.
Adjacency not found	The number of PDUs dropped at both Level-1 and Level-2 because there is no valid adjacency on the interface where they were received. This counter will only be displayed if it has a value greater than zero.
Adjacency Level Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the adjacency from which the PDU is received has a different level than the PDU level. This counter will only be displayed if it has a value greater than zero.
IS Level Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the IS-IS router level mismatches with the PDU level received. This counter will only be displayed if it has a value greater than zero.
Length Too Short	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU length is less than the standard PDU header length. This counter will only be displayed if it has a value greater than zero.
Length Too Long	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU length is greater than the MTU of the link. This counter will only be displayed if it has a value greater than zero.
Max Area Check Failure	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a maximum area count different than what is configured on this IS-IS router. This counter will only be displayed if it has a value greater than zero.
Zero Checksum	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a zero checksum. This counter will only be displayed if it has a value greater than zero.
Checksum Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a checksum different than the computed checksum on the received PDU. This counter will only be displayed if it has a value greater than zero.
Invalid Length	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a different length than what is advertised in the PDU header. This counter will only be displayed if it has a value greater than zero.

## Examples

This example displays sample output from the **show isis counts** command.

```
device# show isis counts

Area Mismatch: 0
Max Area Mismatch: 0
System ID Length Mismatch: 0
LSP Sequence Number Skipped: 0
LSP Max Sequence Number Exceeded: 0
Level-1 Database Overload: 0
Level-2 Database Overload: 0
Our LSP Purged: 0
```

show isis counts

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis database

Displays information about the entries in the LSP database.

## Syntax

```
show isis database lsp-id
show isis database detail [ level1 | level2 ]
show isis database level1
show isis database level2
show isis database summary
```

## Parameters

<b>lsp-id</b>	Specifies a link-state packet (LSP) in HHHH.HHHH.HHHH.HH-HH format, for example, 3333.3333.3333.00-00, or by entering a name, for example, XMR.00-00.
<b>detail</b>	Specifies detailed information.
<b>level1</b>	Specifies Level 1 packets only.
<b>level2</b>	Specifies Level 2 packets only.
<b>summary</b>	Specifies summarized information.

## Modes

Privileged EXEC mode

## Command Output

The **show isis database** command displays the following information:

Output field	Description
LSPID	The LSP ID, which consists of the source ID (6 bytes), the pseudonode (1 byte), and LSPID (1 byte).  <b>NOTE</b> If the address has an asterisk ( * ) at the end, this indicates that the LSP is locally originated.
LSP Seq Num	The sequence number of the LSP.
LSP Checksum	The checksum calculated by the device that sent the LSP and used by the device to verify that the LSP was not corrupted during transmission over the network.

Output field	Description
LSP Holdtime	The maximum number of seconds during which the LSP will remain valid.  <b>NOTE</b> The IS that originates the LSP sets the timer for the LSP. As a result, LSPs do not all have the same amount of time remaining when they enter the device's LSP database.
ATT	A 4-bit value extracted from bits 4 - 7 in the Attach field of the LSP.
P	The value in the Partition option field of the LSP. The field can have one of the following values: <ul style="list-style-type: none"> <li>• 0 - The IS that sent the LSP does not support partition repair.</li> <li>• 1 - The IS that sent the LSP supports partition repair.</li> </ul>
OL	The value in the LSP database overload field of the LSP. The field can have one of the following values: <ul style="list-style-type: none"> <li>• 0 - The overload bit is off.</li> <li>• 1 - The overload bit is on, indicating that the IS that sent the LSP is overloaded and should not be used as a IS-IS transit router for that level.</li> </ul>
NLPID	The Network Layer Protocol Identifier (NLPID), which specifies the protocol the IS that sent the LSP is using. Usually, this value is "CC(IP)".
IP address	The IP address of the interface that sent the LSP. The device can use this address as the next hop in routes to the addresses listed in the rows below.
Destination addresses	The rows of information below the IP address row are the destinations advertised by the LSP. The device can reach these destinations by using the IP address listed above as the next hop.  Each destination entry contains the following information: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Device type - The device type at the destination. The type can be one of the following: <ul style="list-style-type: none"> <li>- End System - The device is an ES.</li> <li>- IP-Internal - The device is an ES within the current area. The IP address and subnet mask are listed.</li> <li>- IS - The device is another IS. The NET (NSAP address) is listed.</li> <li>- 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.</li> <li>- 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.</li> </ul> </li> </ul>
Flooding to <i>num</i> interface:	Identifies the number of interfaces on which the specific LSP entry will be flooded and identifies the interfaces.
Acking to <i>num</i> interface:	Identifies the number of interfaces on which the specific LSP entry will be acknowledged and identifies the interfaces.



## Examples

The following is sample output for the **show isis database** command when no argument or keyword is used.

```
device# show isis database

IS-IS Level-1 Link State Database
LSPID                               Seq Num   Checksum  Holdtime ATT/P/OL
R1.00-00*                            0x00000030 0x163a    394      0/0/0
IS-IS Level-2 Link State Database
LSPID                               Seq Num   Checksum  Holdtime ATT/P/OL
R1.00-00*                            0x00000030 0xc865    394      0/0/0
```

The following is sample output for the **show isis database** command when the **detail** keyword is used.

```
device# show isis database detail

IS-IS Level-1 Link State Database
LSPID                               Seq Num   Checksum  Holdtime ATT/P/OL
R1.00-00*                            0x00000038 0x0642    1095     0/0/0
  Area Address: 11
  NLPID: IP
  Hostname: R1
  Metric: 10      IP-Internal 1.2.3.4/32      Up: 0
  Metric: 10      IP-Internal 11.2.1.16/30   Up: 0
  Metric: 10      IP-Internal 11.2.1.0/30    Up: 0
  Metric: 10      IP-Internal 11.2.1.8/30    Up: 0
  Metric: 10      IP-Internal 11.2.1.4/30    Up: 0
  Metric: 10      IP-Internal 11.2.1.12/30   Up: 0
  Metric: 10      IP-Internal 11.2.1.24/30   Up: 0
  Metric: 10      IP-Internal 11.2.1.20/30   Up: 0
  Metric: 10      IP-Internal 11.2.1.32/30   Up: 0
  Metric: 10      IP-Internal 11.2.1.28/30   Up: 0
  Metric: 10      IP-Internal 11.2.1.36/30   Up: 0
  Metric: 10      IS 76:8e:f8:5:58:12. 2
  Metric: 10      IS 76:8e:f8:5:58:12. 3
  Metric: 10      IS 76:8e:f8:5:58:12. 4
  Metric: 10      IS 76:8e:f8:5:58:12. 5
  Metric: 10      IS 76:8e:f8:5:58:12. 6
  Metric: 10      IS 76:8e:f8:5:58:12. 7
  ...
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis hostname

Displays the router-name-to-system-ID mapping table entries for an IS-IS device.

## Syntax

`show isis hostname`

## Modes

Privileged EXEC mode

## Examples

This example displays sample output from the `show isis hostname` command.

```
device# show isis hostname

Total number of entries in IS-IS Hostname Table: 1
System ID      Hostname      * = local IS
-----
* 768e.f805.5812  R1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis interface

Displays information about IS-IS interfaces for a device.

## Syntax

**show isis interface**

**show isis interface brief**

**show isis interface ethernet** *slot/port*

**show isis interface loopback** *number*

**show isis interface ve** *vlan\_id*

## Parameters

**brief**

Specifies a brief summary of IP interface IS-IS interface information.

**ethernet** *slot / port*

Specifies an Ethernet slot and port.

**loopback** *number*

Specifies a loopback interface. Valid values range from 1 through 255.

**ve** *vlan\_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

## Modes

Privileged EXEC mode

## Command Output

The **show isis interface** command displays the following information:

Output field	Description
Total number of IS-IS interfaces	The number of interfaces on which IS-IS is enabled.
Interface	The port or virtual interface number to which the information listed below applies.
Circuit State	The state of the circuit, which can be one of the following: <ul style="list-style-type: none"> <li>DOWN</li> <li>UP</li> </ul>
Circuit Mode	The IS-IS type in use on the circuit. The mode can be one of the following: <ul style="list-style-type: none"> <li>LEVEL-1</li> <li>LEVEL-2</li> <li>LEVEL-1-2</li> </ul>

Output field	Description
Circuit Type	The type of IS-IS circuit running on the interface. The circuit type can be one of the following: <ul style="list-style-type: none"> <li>• BCAST (broadcast).</li> <li>• PTP (Point-to-Point)</li> </ul>
Passive State	The passive state determines whether the interface is allowed to form an IS-IS adjacency with the IS at the other end of the circuit. The state can be one of the following: <ul style="list-style-type: none"> <li>• FALSE - The passive option is disabled. The interface can form an adjacency with the IS at the other end of the link.</li> <li>• TRUE - The passive option is enabled. The interface cannot form an adjacency, but can still advertise itself into the area.</li> </ul>
Circuit Number	The ID that the instance of IS-IS running on the interface applied to the circuit between this interface and the interface at the other end of the link.
MTU	The maximum length supported for IS-IS PDUs sent on this interface.
Level-1 Auth-mode	One of the following authentication modes set for Level-1 on the router: <ul style="list-style-type: none"> <li>• None</li> <li>• md5</li> <li>• cleartext</li> </ul>
Level-2 Auth-mode	One of the following authentication modes set for Level-2 on the router: <ul style="list-style-type: none"> <li>• None</li> <li>• md5</li> <li>• cleartext</li> </ul> <p>This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.</p>
Level-1 Metric	The default-metric value that the device inserts in IS-IS Level-1 PDUs for this interface.
Level-1 Priority	The priority of this IS to be elected as the Designated IS for Level-1 in this broadcast network.
Level-1 Hello Interval	The number of seconds the software waits between sending Level-1 hello PDUs to the IS at the other end of the circuit.
Level-1 Hello Multiplier	The number by which the software multiplies the hello interval to calculate the hold time set in Level-1 Hello PDUs sent on the circuit.
Level-1 Designated IS	The NET of the Level-1 Designated IS.
Level-1 DIS Changes	The number of times the NET of the Level-1 Designated IS has changed.
Level-2 Metric	The default-metric value that the device inserts in IS-IS Level-2 PDUs for this interface.
Level-2 Priority	The priority of this IS to be elected as the Designated IS for Level-2 in this broadcast network.
Level-2 Hello Interval	The number of seconds the software waits between sending Level-2 Hello messages to the IS at the other end of the circuit.

Output field	Description
Level-2 Hello Multiplier	<p>The number by which the software multiplies the hello interval to calculate the hold time set for Level-2 Hello PDUs sent on this circuit.</p> <p>This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.</p>
Level-2 Designated IS	The NET of the Level-2 Designated IS.
Level-2 DIS Changes	The number of times the NET of the Level-2 Designated IS has changed.
Next IS-IS LAN Level-1 Hello	Number of seconds before next Level-1 Hello PDU will be transmitted by the device.
Next IS-IS LAN Level-2 Hello	Number of seconds before next Level-2 Hello PDU will be transmitted by the device.
Number of active Level-1 adjacencies	The number of ISs with which this interface has an active Level-1 adjacency.
Number of active Level-2 adjacencies	The number of ISs with which this interface has an active Level-2 adjacency.
Circuit State Changes	The number of times the state of the circuit has changed.
Circuit State Adjacencies Changes	The number of times an adjacency has started or ended on this circuit.
Rejected Adjacencies	The number of adjacency attempts by other ISs rejected by the device.
Circuit Authentication L1 failures	The number of times the device rejected a circuit because the authentication did not match the authentication configured for Level 1 on the device.
Circuit Authentication L2 failures	<p>The number of times the device rejected a circuit because the authentication did not match the authentication configured for Level 2 on the device.</p> <p>This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.</p>
Bad LSP	<p>The number of times the interface received a bad LSP from an IS at the other end of the circuit. The following conditions can cause an LSP to be bad:</p> <ul style="list-style-type: none"> <li>• Invalid checksum</li> <li>• Invalid length</li> <li>• Invalid lifetime value</li> </ul>
Control Messages Sent	The number of IS-IS control PDUs sent on this interface.
Control Messages Received	The number of IS-IS control PDUs received on this interface.
Hello Padding:	<p>The Hello Padding configuration, which can be:</p> <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
IP Enabled	If set to TRUE, the IP protocol is enabled for this circuit.
IP Address and Subnet Mask	The IP address and subnet mask for this interface.

show isis interface

Output field	Description
IPv6 Enabled	If set to TRUE, the IPv6 protocol is enabled for this circuit.
IPv6 Address and Subnet Mask	The IPv6 address and subnet mask for this interface.
IPv6 Link-Local Addresses	The IPv6 link local address for this interface.
MPLS TE Enabled:	If set to TRUE, MPLS Traffic Engineering protocol is enabled for this circuit.
BFD Enabled:	If set to TRUE, BiDirectional Forwarding Detection is enabled for this circuit.

## Examples

The following example displays information about IS-IS interfaces for a device.

```

device# show isis interface
Total number of IS-IS Interfaces: 11

Interface: Ve 301
  Circuit State: UP Circuit Mode: Level 1-2
  Circuit Type: BCAST Passive State: FALSE
  Circuit Number: 2, MTU: 1500
  Level-1 Auth-mode: NONE
  Level-2 Auth-mode: NONE
  Level-1 Metric: 10, Level-1 Priority: 64
  Level-1 Hello Interval: 10, Level-1 Hello Multiplier: 3
  Level-1 Designated IS: R1-02 Level-1 DIS Changes: 2
  Level-2 Metric: 10, Level-2 Priority: 64
  Level-2 Hello Interval: 10, Level-2 Hello Multiplier: 3
  Level-2 Designated IS: R1-02 Level-2 DIS Changes: 2
  Next IS-IS LAN Level-2 Hello in 11 seconds
  Number of active Level-2 adjacencies: 0
  Next IS-IS LAN Level-1 Hello in 1 seconds
  Number of active Level-1 adjacencies: 0
  Circuit State Changes: 1 Circuit Adjacencies State Changes: 0
  Rejected Adjacencies: 0
  Circuit Authentication L1 failures: 0
  Circuit Authentication L2 failures: 0
  Bad LSPs: 0
  Control Messages Sent: 7577 Control Messages Received: 0
  Hello Padding: Enabled
  IP Enabled: TRUE
  IP Addresses:
    11.2.1.1/30
  IPv6 Enabled: FALSE
  MPLS TE Enabled: FALSE
  BFD Enabled: FALSE
  LDP-SYNC: Disabled, State:

Interface: Ve 302
  Circuit State: UP Circuit Mode: Level 1-2
  Circuit Type: BCAST Passive State: FALSE
  Circuit Number: 3, MTU: 1500
  Level-1 Auth-mode: NONE
  Level-2 Auth-mode: NONE
  Level-1 Metric: 10, Level-1 Priority: 64
  Level-1 Hello Interval: 10, Level-1 Hello Multiplier: 3
  Level-1 Designated IS: R1-03 Level-1 DIS Changes: 2
  Level-2 Metric: 10, Level-2 Priority: 64
  Level-2 Hello Interval: 10, Level-2 Hello Multiplier: 3
  Level-2 Designated IS: R1-03 Level-2 DIS Changes: 2
  Next IS-IS LAN Level-2 Hello in 2 seconds
  Number of active Level-2 adjacencies: 0
  Next IS-IS LAN Level-1 Hello in 4 seconds
  Number of active Level-1 adjacencies: 0
  Circuit State Changes: 1 Circuit Adjacencies State Changes: 0
  Rejected Adjacencies: 0
  Circuit Authentication L1 failures: 0
  Circuit Authentication L2 failures: 0
  Bad LSPs: 0
  Control Messages Sent: 7600 Control Messages Received: 0
  Hello Padding: Enabled
  IP Enabled: TRUE
  IP Addresses:
    11.2.1.5/30
  IPv6 Enabled: FALSE
  MPLS TE Enabled: FALSE
  BFD Enabled: FALSE
  LDP-SYNC: Disabled, State:
...

```

show isis interface

The following example displays summarized information about IS-IS interfaces for a device.

```
device# show isis interface brief
```

```
Total number of IS-IS Interfaces: 11
Interface      Type  State Mode Passive MTU  UpAdj DIS  StateChg  AdjStateChg
Ve 301         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 302         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 303         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 304         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 305         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 306         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 307         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 308         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 309         BCAST UP   L12  FALSE 1500 0    None 1      0
Ve 310         BCAST UP   L12  FALSE 1500 0    None 1      0
Lo 1           BCAST UP   L12  TRUE  0     0    None 1      0
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show isis neighbors

Displays IS-IS neighbor information.

## Syntax

```
show isis neighbor [ detail ]
```

## Parameters

**detail**

Specifies detailed information.

## Modes

Privileged EXEC mode

## Command Output

The **show isis neighbors** command displays the following information:

Output field	Description
Total number of IS-IS Neighbors	The number of ISs with which the device has formed IS-IS adjacencies.
System ID	The System ID of the neighbor or the hostname of the neighbor.
Interface	The device port or virtual interface attached to the neighbor.
SNPA	The Subnetwork Point of Attachment (SNPA), which is the MAC address of the device port or virtual interface attached to the neighbor.
State	The state of the adjacency with the neighbor. The state can be one of the following: <ul style="list-style-type: none"> <li>DOWN - The adjacency is down.</li> <li>INIT - The adjacency is being established and is not up yet.</li> <li>UP - The adjacency is up.</li> </ul>
Holdtime	The neighbor's advertised hold time.
Type	The IS-IS type of the adjacency. The type can be one of the following: <ul style="list-style-type: none"> <li>ISL1 - Level-1 IS</li> <li>ISL2 - Level-2 IS</li> <li>ES - ES</li> </ul> <p><b>NOTE</b> The device forms a separate adjacency for each IS-IS type. Thus, if the device has both types of IS-IS adjacencies with the neighbor, the display contains a separate row of information for each adjacency.</p>
Pri	The priority of this IS to be elected as the Designated IS in this broadcast network.

Output field	Description
StateChgeTime	The amount of time that has passed since the adjacency last changed state.
Protocol	The routing protocol supported by the neighbor. The protocol can be one of the following: <ul style="list-style-type: none"> <li>• MT-ISIS - Multi-Topology is enabled on the neighbor.</li> <li>• ISIS - Multi-Topology is not enabled on the neighbor.</li> </ul>

The **show isis neighbors detail** command displays the following information:

Output field	Description
Total number of IS-IS Neighbors	The number of ISs with which the device has formed IS-IS adjacencies.
System ID	The System ID of the neighbor or the hostname of the neighbor.
Interface	The device port or virtual interface attached to the neighbor.
SNPA	The Subnetwork Point of Attachment (SNPA), which is the MAC address of the device port or virtual interface attached to the neighbor.
State	The state of the adjacency with the neighbor. The state can be one of the following: <ul style="list-style-type: none"> <li>• DOWN - The adjacency is down.</li> <li>• INIT - The adjacency is being established and is not up yet.</li> <li>• UP - The adjacency is up.</li> </ul>
Holdtime	The neighbor's advertised hold time.
Type	The IS-IS type of the adjacency. The type can be one of the following: <ul style="list-style-type: none"> <li>• ISL1 - Level-1 IS</li> <li>• ISL2 - Level-2 IS</li> <li>• ES - ES</li> </ul> <p><b>NOTE</b> The device forms a separate adjacency for each IS-IS type. Thus, if the device has both types of IS-IS adjacencies with the neighbor, the display contains a separate row of information for each adjacency.</p>
Pri	The priority of this IS to be elected as the Designated IS in this broadcast network.
StateChgeTime	The amount of time that has passed since the adjacency last changed state.
3-Way Handshake TLV received	The received 3-way handshake TLV for the interface.
Area Address (es)	The address of the area.
Protocols Supported	The topology supported by the neighbor.
IP Address	The IP address assigned to the neighbor interface.
Adj Usage L1	The adjacency level used by the neighbor.
circuit ID	The ID of the IS-IS circuit running on the neighbor interface.
Protocol	The routing protocol supported by the neighbor. The protocol can be one of the following: <ul style="list-style-type: none"> <li>• MT-ISIS - Multi-Topology is enabled on the neighbor.</li> <li>• ISIS- Multi-Topology is not enabled on the neighbor.</li> </ul>

## Examples

The following example displays information about IS-IS neighbors.

```
device# show isis neighbors
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis routes

Displays the routes in the IS-IS route table.

## Syntax

```
show isis routes [ ip-address subnet-mask | ip-address/prefix ]
```

## Parameters

*ip-address subnet-mask*

Specifies an IP address and network mask.

*ip-address/prefix*

Specifies an IP address and prefix.

## Modes

Privileged EXEC mode

## Command Output

The **show isis routes** command displays the following information:

Output field	Description
Total number of IS-IS routes	The total number of routes in the device's IS-IS route table. The total includes Level-1 and Level-2 routes.
Destination	The IP destination of the route.
Mask	The subnet mask for the destination address.
Cost	The IS-IS default metric for the route, which is the cost of using this route to reach the next-hop router to this destination.
Type	The route type, which can be one of the following: <ul style="list-style-type: none"> <li>• L1 - Level-1 route</li> <li>• L2 - Level-2 route</li> </ul>
Tag	The tag value associated with the route.
Path	The path number in the table. The IS-IS route table can contain multiple equal-cost paths to the same destination, in which case the paths are numbered consecutively. When IP load sharing is enabled, the device can load balance traffic to the destination across the multiple paths.
Next Hop IP	The IP address of the next-hop interface to the destination.
Interface	The device interface (port or virtual interface) attached to the next hop.
Flags	Values used by technical support for troubleshooting.

## Examples

The following is sample output for the **show isis routes** command when no argument or keyword is used.

```
device# show isis routes
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show isis spf-log

Displays IS-IS link-state packet (LSP) logging information.

## Syntax

```
show isis spf-log
```

```
show isis spf-log detail
```

```
show isis spf-log level-1 [detail ]
```

```
show isis spf-log level-2 [detail ]
```

## Parameters

**detail**

Specifies detailed information.

**level-1**

Specifies Level 1 packets only.

**level-2**

Specifies Level 2 packets only.

## Modes

Privileged EXEC mode

## Command Output

The **show isis spf-log** command displays the following information:

Output field	Description
When	When (in hours: minutes : seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	The time required to complete this SPF run. Elapsed time is normal clock time (not CPU time). Other options for this field are: <ul style="list-style-type: none"> <li>Running - the SPF is still running and the duration will be updated after the SFP has run.</li> <li>Pending - the event is pending and another SPF will be run once the currently executing SPF has completed.</li> </ul>
Nodes	The number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	The number of events that triggered this SPF run. When a topology change has occurred, multiple link-state packets (LSPs) are received in a short time. Since a router waits about 5 seconds before running a full SPF run, it can include all new information. This count includes the number of events (such as receiving new LSPs) that occurred while the router was waiting the 5 second interval before running full SPF.

Output field	Description
Last Trigger LSP	When a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue about the source of routing instability in an area. If multiple LSPs in a single level are causing SPF runs, only the LSP ID of the last received LSP is recorded.
Triggers	The reason that a full SPF calculations was triggered.
Alternate Route Check	PSPF deleted an IPv4 or IPv6 route. Full SPF must run to find the alternate route.
Route Change in L1 SPF Run	The L1 SPF run added or deleted an IPv4 or IPv6 route. The L2 SPF must run to accommodate this change.
LSP Purged	An LSP was purged. A full SPF calculation must process this change.
LSP Added	A new LSP has appeared in the database. A full SPF calculation is needed to process this new LSP.
Summary Address Change	A summary address configuration change has occurred.
Adjacency State Change	An adjacency was added or deleted.
Admin Distance Change	The administrative distance configuration has changed.
LSP Header Change	The LSP header (attached or overload bits) is changed.
IS Neighbor TLV Change	An IS neighbor TLV was added or deleted in an LSP.
Area Address TLV Change	The area address TLV changed.
Interface IP Address Change	The IP address configuration changed.
IP Address TLV Change	An IP address TLV changed in the LSP.
IPv6 Address TLV Change	An IPv6 address TLV changed in the LSP.
IS-IS Level Change	The IS-IS level configuration changed.
Interface Metric Change	The IS-IS interface metric configuration changed.
LSP Changed - PSPF Disabled	The LSP changed and PSPF is disabled.
LSP Overload Bit Change	The overload bit in the LSP header changed.
Interface State Change	The interface state changed to up or down.
Redist Prefix-List Change	The redistribution list configuration changed.
Redist Policy Change	The redistribution policy configuration changed.
Maximum Path Change	The IS-IS maximum path configuration changed.
IP Load Sharing Change	The IP load sharing configuration changed.
User Cleared IS-IS Route	The user cleared a specific IS-IS route.
User Cleared IS-IS Routes	The user cleared all IS-IS routes.
Neighbor NLPID Change	NLPID set is changed in received hellos.
ISIS Enable	IS-IS was enabled.
ISTCT_SPF Computation	The user issued the <b>disable-incremental-stct-spf-opt</b> command.
User Cleared IS-IS All	The user issued the <b>clear isis all</b> command.
Interface Config Change	ISIS was enabled or disabled on a port.
User Trigger	The user issued the <b>clear isis spf-trigger</b> command.
Recompute InterLeve Routes	The neighbor IS-type is changed either from L1 to L12 or L12 to L1
Exited Overload State	IS-IS exited from an overload condition.

## Examples

The following is sample output for the **show isis spf-log** command.

```
device# show isis spf-log
ISIS Level-1 SPF Log
  When      Duration Nodes Count Last-Trigger-LSP      Trigger
  10h34m13s 0ms      1    10   R1.00-00             Interface State Change
  10h34m38s 0ms      1    2    R1.00-00             Interface Config Change
  10h34m43s 0ms      1    18   R1.00-00             Interface Config Change
  10h34m48s 0ms      1    5    R1.00-00             Interface State Change
ISIS Level-2 SPF Log
  When      Duration Nodes Count Last-Trigger-LSP      Trigger
  10h34m13s 0ms      1    10   R1.00-00             Interface State Change
  10h34m38s 0ms      1    2    R1.00-00             Interface Config Change
  10h34m43s 0ms      1    18   R1.00-00             Interface Config Change
  10h34m48s 0ms      1    5    R1.00-00             Interface State Change
```

The following is sample output for the **show isis spf-log** command when the **detail** keyword is used.

```
device# show isis spf-log detail

ISIS Level-1 SPF Log
  When      Duration Nodes Count Last-Trigger-LSP      Trigger
  12h18m45s 0ms      1    10   R1.00-00             Interface State Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
    First Trigger: 12h18m50s Ve 305 State Changed to Up
  12h19m10s 0ms      1    2    R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
    First Trigger: 12h19m15s Ve 310 State Changed to Down
  12h19m15s 0ms      1    18   R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
    First Trigger: 12h19m18s Ve 301 State Changed to Down
  12h19m20s 0ms      1    5    R1.00-00             Interface State Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
    First Trigger: 12h19m25s LSP R1.00-00 Area Address TLV Changed
ISIS Level-2 SPF Log
  When      Duration Nodes Count Last-Trigger-LSP      Trigger
  12h18m45s 0ms      1    10   R1.00-00             Interface State Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
    First Trigger: 12h18m50s Ve 305 State Changed to Up
  12h19m10s 0ms      1    2    R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
    First Trigger: 12h19m15s Ve 310 State Changed to Down
  12h19m15s 0ms      1    18   R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
    First Trigger: 12h19m18s Ve 301 State Changed to Down
  12h19m20s 0ms      1    5    R1.00-00             Interface State Change
...
```

The following is sample output for the **show isis spf-log** command when the **level-1** keyword is used.

```
device# show isis spf-log level-1
ISIS Level-1 SPF Log
  When      Duration Nodes Count Last-Trigger-LSP      Trigger
  12h19m40s 0ms      1    10   R1.00-00             Interface State Change
  12h20m5s 0ms      1    2    R1.00-00             Interface Config Change
  12h20m10s 0ms      1    18   R1.00-00             Interface Config Change
  12h20m15s 0ms      1    5    R1.00-00             Interface State Change
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show isis traffic

Displays information about IS-IS packet counts.

## Syntax

```
show isis traffic
```

## Modes

Privileged EXEC mode

## Command Output

The **show isis traffic** command displays the following information:

Output field	Description
Level-1 Hellos	The number of Level-1 hello PDUs sent and received by the device.
Level-2 Hellos	The number of Level-2 hello PDUs sent and received by the device.
Level-1 LSP	The number of Level-1 link-state PDUs sent and received by the device.
Level-2 LSP	The number of Level-2 link-state PDUs sent and received by the device.
Level-1 CSNP	The number of Level-1 Complete Sequence Number PDUs (CSNPs) sent and received by the device.
Level-2 CSNP	The number of Level-2 CSNPs sent and received by the device.
Level-1 PSNP	The number of Level-1 Partial Sequence Number PDUs (PSNPs) sent and received by the device.
Level-2 PSNP	The number of Level-2 PSNPs sent and received by the device.

## Examples

The following is sample output for the **show isis traffic** command.

```
device# show isis traffic
```

```

Level-1 Hellos           Message Received   Message Sent
Level-2 Hellos           0                  44912
PTP Hellos               0                  44927
Level-1 LSP              0                  0
Level-2 LSP              0                  0
Level-1 CSNP             0                  0
Level-2 CSNP             0                  0
Level-1 PSNP             0                  0
Level-2 PSNP             0                  0
```

show isis traffic

## History

Release version	Command history
16r.1.00	This command was introduced.

# show port-security

Displays the configuration information related to port security.

## Syntax

```
show port-security [ addresses | interface ethernet slot/port ]
```

## Modes

Privileged EXEC mode

Interface configuration mode

## Command Output

The **show port-security** command displays the following information:

Output field	Description
Secure Port	The port on which port MAC security is enabled.
MaxSecureAddress (count)	The maximum limit for the number of secure MAC addresses allowed on the interface.
StaticSec (count)	The number of MAC addresses that are manually configured.
Violated	The status that shows whether the port security violation has occurred.
Action	The configured response action that will be taken when a port security violation occurs.
Sticky	The status that shows whether sticky MAC learning is enabled.
Port Security	The status that shows whether port MAC security is enabled.
Port Status	The status of the port.
Violation Mode	The configured response action that will be taken when a port security violation occurs.
Violated	The status that shows whether the port security violation has occurred.
Sticky Enabled	The status that shows whether sticky MAC learning is enabled.
Maximum MAC addresses	The maximum limit for the number of secure MAC addresses allowed on the interface.
Total MAC addresses	The total number of secure MAC addresses learned on the interface.
Configured MAC addresses	The total number of secure MAC addresses configured on the interface manually.
Last violation time	The time when the last port security violation occurred.
Shutdown time (in Minutes)	The configured auto recovery time for port security violation.
Vlan	The VLAN to which the port is mapped.
Mac-address	The secured MAC address.
Type	The types of secure MAC addresses that are used in port MAC security.
Ports	The port on which port MAC security is enabled.

## Examples

To display the port MAC security configuration details across ports on the device, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security
Secure      MaxSecureAddr  CurrentAddr  StaticSec  Violated  Action  Sticky
Port        (count)        (count)      (count)
Eth 3/2     10              0             1          No        Shutdown No
```

To display the statistics of the port MAC security configured for an interface, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security interface ethernet 3/2
Port Security           : Enabled
Port Status             : Up
Violation Mode          : Shutdown
Violated                 : No
Sticky Enabled          : No
Maximum MAC addresses   : 10
Total MAC addresses     : 0
Configured MAC addresses : 1
Last violation time     :
Shutdown time (in Minutes) : 0
```

To list the secure MAC addresses configured on the device, enter the following command.

```
device(conf-if-eth-3/2)# do show port-security addresses
Secure Mac Address Table
-----
Vlan      Mac-address      Type              Ports
250       3200.1110.0002   Secure-Static     Eth 3/2
```

# Show J through Show Z

---

## show lldp interface

Displays the LLDP status on the specified interface.

### Syntax

```
show lldp interface [ ethernet slot/port ]
```

### Parameters

**ethernet**

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

*slot*

Specifies a valid slot number.

*port*

Specifies a valid port number.

### Modes

Privileged EXEC mode

### Usage Guidelines

If the **ethernet** *slot/port* parameter is not specified, this command displays the LLDP status information received on all the interfaces.

## Examples

To display all the LLDP ethernet interface information, enter the following:

```
device# show lldp interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
 1/1
 1/2
 1/3
 1/4
 1/5
 1/6
 1/8
 1/9
 1/10
 1/11
 1/12
 1/13
 1/14
 1/15
 1/16
 1/17
 1/18
 1/19
 1/20
 1/21
 1/22
 1/23
```

To display the LLDP interface information for a specified ethernet interface, enter the following:

```
device# show lldp interface ethernet 1/18
LLDP information for Eth 1/18
  State:                Enabled
  Mode:                 Receive/Transmit
  Advertise Transmitted: 30 seconds
  Hold time for advertise: 120 seconds
  Tx Delay Timer:      1 seconds
  Transmit TLVs:       Chassis ID          Port ID
                       TTL                Port Description
                       System Name
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show lldp neighbors

Displays LLDP information for all neighboring devices on the specified interface.

## Syntax

```
show lldp neighbors [ interface [ethernet slot/port ]] [detail]
```

## Parameters

### ethernet

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

### slot

Specifies a valid slot number.

### port

Specifies a valid port number.

### detail

Specifies the details of the LLDP neighbor information.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display LLDP information for all neighboring devices on the specified interface.

## Examples

To display LLDP neighbor information on a specific interface, enter the following:

```
device# show lldp neighbors interface ethernet 1/18
Local Port  Dead Interval  Remaining Life  Remote Port ID  Remote Port  Descr  Chassis ID  Tx  Rx
System Name
Eth 1/18    120                115            Ethernet 2/25   Eth 2/25     768e.f807.6000  655 654
R6
```

To display detailed LLDP neighbor information on a specific interface, enter the following:

```
device# show lldp neighbors interface ethernet 1/18 detail
Neighbors for Interface Eth 1/18

MANDATORY TLVs
=====
Local Interface: Eth 1/18 (Local Interface MAC: 768e.f805.5816)
Remote Interface: Ethernet 2/25 (Remote Interface MAC: 768e.f807.610d)
Dead Interval: 120 secs
Remaining Life : 118 secs
Chassis ID: 768e.f807.6000
LLDP PDU Transmitted: 656 Received: 655

OPTIONAL TLVs
=====
Port Interface Description: Eth 2/25
System Name: R6
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show lldp statistics

Displays the LLDP statistics on all interfaces or a specified interface.

## Syntax

```
show lldp statistics [ interface [ethernetslot/port ]]
```

## Parameters

### ethernet

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

### slot

Specifies a valid slot number.

### port

Specifies a valid port number.

## Modes

Privileged EXEC mode

## Usage Guidelines

If you do not specify an interface, this command displays the LLDP statistics for all interfaces.

## Examples

To display LLDP statistics on the specified interface:

```
device# show lldp statistics interface ethernet 1/18
LLDP Interface statistics for Eth 1/18
Frames transmitted: 659
Frames Aged out:    0
Frames Discarded:  0
Frames with Error: 0
Frames Recieved:   657
TLVs discarded:    0
TLVs unrecognized: 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show mac-address-table

Displays MAC address table information.

## Syntax

**show mac-address-table**

**show mac-address-table bridge-domain** [ *id* ]

**show mac-address-table cluster** *cluster-ID* [ { **client** *client-ID* [ **local** | **remote** ] } | **local** | **remote** | { **vlan** *vlan-ID* [ **client** *client-ID* ] } ]

**show mac-address-table count** [ **bridge-domain** *id* ]

**show mac-address-table** [ **address** *mac-address* ] [ **aging-time** ] [ **dynamic** [ **address** *mac-address* ] ] [ **interface ethernet** *slot/port* | **port-channel** *interface number* ] [ **vlan** *vlan id* ] [ **interface ethernet** *slot/port* | **port-channel** *number* | **tunnel** *tunnel id* ] [ **mdb** [ *mac-address* ] | **client** <*client-name*> | **vlan** <*vlan-id*> ] [ **static** [ **address** *mac-address* ] ] [ **interface ethernet** *slot/port* | **port-channel** *number* ] [ **vlan** *vlan id* ] [ **vlan** *vlan id* ]

## Parameters

### **bridge-domain** *id*

Specifies displaying information about MAC addresses learned under a bridge domain. When a bridge domain identifier is not specified, information is displayed about MAC addresses learned under all bridge domains.

### **cluster** *cluster-ID*

Specifies the MCT cluster ID.

### **client** *client-ID*

Specifies the client ID.

### **local**

Displays the local MAC addresses for the cluster or the specified client ID.

### **remote**

Displays the remote MAC addresses for the cluster or the specified client ID.

### **vlan** *vlan-ID*

Specifies the VLAN ID.

### **address** *MAC-address*

Displays forwarding information for a 48-bit MAC address. The valid format is *H.H.H* (available in Privileged EXEC mode only).

### **aging-time**

Displays aging-time.

### **dynamic address** *MAC-address*

Specifies the dynamic MAC addresses for an ethernet interface, port-channel, or VLAN. The valid format is *H.H.H* (available in Privileged EXEC mode only).

### **interface ethernet** *slot/port*

Specifies the ethernet interface with a valid slot number/port number.

**port-channel** *interface number*

Specifies the port channel interface number based on platform.

**port-channel** *number*

Specifies the port channel interface number. The range is from 1 - 512 based on the platform.

**vlan** *vlan id*

Specifies the VLAN interface. The VLAN ID range is from 1 - 4090.

**tunnel** *tunnel id*

Specifies the tunnel interface. The tunnel ID range is from 1 - 100000.

**mdb** *MAC-address*

Specifies the MDB information for the cluster client specific macs. The valid format is *H.H.H* (available in Privileged EXEC mode only).

**client** *client-name*

Displays the client instance. Specify the client name with a maximum of 64 characters.

**static address** *mac-address*

Specifies the static MAC address for an ethernet interface , port-channel, or VLAN. The valid format is *H.H.H* (available in Privileged EXEC mode only).

## Modes

Privileged EXEC mode.

## Usage Guidelines

To display information about MAC addresses learned under all bridge domains, specify the **bridge-domain** option without a bridge-domain identifier.

## Command Output

The **show mac-address-table** command displays the following information:

Output field	Description
Bridge domain	
BD-Id	Bridge domain identifier
Mac-address	MAC address
Type	MAC address type (Dynamic or static)
State	State (Active or Inactive)
Ports	Ethernet or port-channel interfaces
LIF	Logical interface
peer-ip	IP address of a remote VPLS peer

The following example displays the MAC address table aging time.

```
device# show mac-address-table aging-time
MAC Aging-time : 300 seconds
```

show mac-address-table

The following example displays the MAC address table for an MCT cluster.

```
device# show mac-address-table cluster 1
VlanId/BDId  Mac-address      Type      State      Ports/LIF/PW
102 (V)      0001.0001.0001   Dynamic-CCL Active     eth 1/2
102 (V)      0001.0001.0111   Static-CCL Active     po 100
102 (V)      0001.0001.0111   CCR       Active     Eth 3/66
104 (V)      0024.387c.8f00   Dynamic-CCL Active     Po 3
107 (V)      768e.f80b.2801   CR        Active     16.16.16.16
```

## History

Release version	Command history
16r.1.00	This command was introduced.
16r.1.01	Added the MCT cluster and client options.

# show mpls autobw-threshold-table

Displays the global-threshold table with the range of the current-bandwidth and the corresponding absolute adjustment-threshold.

## Syntax

```
show mpls auto-threshold-table
```

## Modes

Operates in all modes.

## Examples

The following example displays the output of the command.

```
device# show mpls autobw-threshold-table
Auto-bandwidth threshold table
Range (kbps)      Threshold (kbps)
0-10              2000
11-1000          3000
1001-10000       5000
10001-max        10000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## show mpls lsp

Displays detailed information about a specific LSP. The underflow-limit parameter and the number of consecutive underflows are displayed. The adjustment-threshold is used from the global table is indicated with the value for current rate. The **show mpls lsp extensive** command shows the adjustment event with the previous rate and the maximum sampled rate.

### Syntax

```
show mpls lsp { lsp_name } [ detail | extensive ]
```

### Parameters

#### detail

Displays information in detail.

#### extensive

Displays information with History.

### Modes

This command operates under all modes.

### Usage Guidelines

### Command Output

The **show mpls lsp** command displays the following information:

Output field	Description
Name	The name of the LSP. LSPs are displayed in alphabetical order.
To	The egress LER for the LSP.
From	The LSPs source address, configured with the <b>from</b> command. When a source IP address has not been specified for the LSP with the from command, and the LSP has not been enabled, then '(n/a)' displays in the 'From' field.
admin	The administrative state of the LSP. Once the user activates the LSP with the <b>enable</b> command, the administrative state changes from DOWN to UP.
status	The operational state of the LSP. This field indicates whether the LSP has been established through signaling and is capable of having packets forwarded through it. When the status of the LSP is DOWN, the reason why the LSP is down is shown in parentheses. There maybe a short period of time after the user enables the LSP that the administrative state of the LSP is UP, but the status is DOWN. Once the LSP has been established through signaling, both the administrative state and the status is UP.
Tunnel interface (primary path)	The path currently selected for this LSP.
Times primary LSP goes up since enabled	The number of times the status of the LSPs primary path transitions from DOWN to UP.
Metric	The metric for the LSP, configured with the <b>metric</b> command.
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.

Output field	Description
active	Specifies if the primary path is active.
Setup priority	The configured setup priority for the LSP.
hold priority	The configured hold priority for the LSP.
Max rate	The maximum rate of packets that can go through the LSP (in kbps), set with the <b>traffic-eng max-rate</b> command.
mean rate	The average rate of packets that can go through the LSP (in kbps), set with the <b>traffic-eng mean-rate</b> command.
mode	Mode displays if the LSP is in monitor-only or monitor-and-signal mode.
adjustment threshold	Displays the configured adjustment-threshold value.
minimum bw	The configured minimum bandwidth.
maximum bw	The configured maximum bandwidth.
overflow limit	Displays the configured overflow-limit value.
underflow limit	The number of samples that have to be below the threshold, to trigger a premature adjustment.
sample-record	Whether the template is set to record the sample history.
Constraint-based routing enabled	Whether CSPF is in effect for the LSP.
Path calculated using constraint-based routing	Whether the explicit path used by the active path was calculated using the constraint-based routing.
Path calculated using interface constraint	Whether the explicit path used by the active path was calculated using the interface-based routing.
Path cost	The total cost of this path.
Tie breaking	The tie-breaking method CSPF uses to select a path from a group of equal-cost paths to the egress LER, set with the <b>tie-breaking</b> command.
LDP tunnel enabled	If LDP tunneling is enabled, the line reads "yes". If it is not enabled, the line reads "no".
Soft preemption enabled	Soft preemption minimizes traffic disruptions and gracefully reroutes the preempted LSPs.
Sec. path	The name of the secondary path for this LSP and whether the path is currently active.
active	Displays if the secondary path is active.
Hot-standby	Whether the secondary path is a hot-standby path.
status	The operational state of the secondary path
Setup priority	The configured setup priority for the LSP.
hold priority	The configured hold priority for the LSP
Max rate	The maximum rate of packets that can go through the LSP (in kbps), set with the <b>traffic-eng max-rate</b> command.
mean rate	The average rate of packets that can go through the LSP (in kbps), set with the <b>traffic-eng mean-rate</b> command.
max burs	The maximum size (in bytes) of the largest burst the LSP can send at the maximum rate, set with the <b>traffic-eng max-burst</b> command.
mode	Mode shows if the LSP is in monitor-only or monitor-and-signal mode.
adjustment threshold	Displays the configured adjustment-threshold value.
minimum bw	The configured minimum bandwidth.
maximum bw	The configured maximum bandwidth.
overflow limit	Displays the configured overflow-limit value.
underflow limit	The number of samples which must be below the threshold to trigger a premature adjustment.
sample-record	Whether the template is set to record the sample history.
Constraint-based routing enabled	Whether CSPF is in effect for the LSP.

Output field	Description
hop limit	The maximum number of hops a path calculated by CSPF can have, set with the <b>hop-limit</b> command.
Soft preemption enabled	Soft preemption minimizes traffic disruptions and gracefully reroutes the preempted LSPs
Active path attributes	
Tunnel interface	The MPLS tunnel interface port ID.
outbound interface	The outbound label used by the active path of the LSP.
Tunnel index	The tunnel index for the active path of the LSP.
Tunnel instance	
outbound label	The outbound label used by the active path of the LSP.
Auto-bandwidth running info mode	
adjustment interval	Displays the configured adjustment-timer value.
adjustment threshold	Displays the configured adjustment-threshold value.
overflow limit	Displays the configured overflow-limit value.
underflow limit	The number of samples that must be below the threshold to trigger a premature adjustment.
minimum bw	The configured minimum bandwidth.
maximum bw	The configured maximum bandwidth.
Samples collected	Number of samples collected so far in the current adjustment-interval.
max sampled bw	The maximum number of the samples collected so far in the current adjustment-interval.
last sample	The last sampled-bandwidth.
Sample-record	Whether the template is set to record the sample history.
adjustment due in	Displays the time remaining for the current adjust-interval to expire.
Adjustment ignored	This consecutive number of times the adjustment was ignored due to any reason.
Current bandwidth	Current running bandwidth.
Recorded routes	The addresses recorded by the RECORD_ROUTE object during RSVP signaling.



## Examples

The following example shows the output of the command, specifying the LSP *name* with the **extensive** option.

```
device# show mpls lsp extensive
LSP lsp1, to 10.23.23.23
  From: 10.34.34.34, 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: templatel, mode: monitor-only adjustment interval: 86400 sec, adjustment
threshold: 0 minimum bw: 0 kbps, maximum bw: 2147483647 kbps
  overflow limit: 0, underflow limit: 20, sample-record: disabled
  Constraint-based routing enabled: yes
  Path calculated using constraint-based routing: yes
  Path calculated using interface constraint: no
  Path cost: 20
  Tie breaking: random, hop limit: 0
  LDP tunneling enabled: no
  Soft preemption enabled: no
  Sec. path: vial6, 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
  10.31.31.16 -> 10.161.161.1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show mpls policy

Use the show mpls policy command to view the current policy.

## Syntax

```
show mpls policy
```

## Modes

Privileged EXEC mode.

## Examples

The following example shows a sample output of the command.

```
device# show mpls policy
Current MPLS policy settings:
  CSPP interface constraint: disabled
  CSPP-Group computation-mode: disabled
  CSPP computation-mode:
    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
  Transit session accounting: disabled
  Polling interval for MPLS LSP traffic statistics: 300 seconds
  Advertise TE parameters via: none
  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
  Soft preemption cleanup-timer: 30 seconds
  MPLS TE Periodic Flooding Timer : 180 seconds
  MPLS TE flooding thresholds
    Global UP thresholds : None
    Global DOWN thresholds : None
    Default UP thresholds : 15 30 45 60 75 80 85 90 95 96 97 98 99 100
    Default DOWN thresholds : 99 98 97 96 95 90 85 80 75 60 45 30 15
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show mpls rsvp

Displays RSVP information.

## Syntax

```
show mpls rsvp [ igp-sync [ link [ detail | ip ip_addr ] ] | lsp [ detail | name name ] ] | interface [ detail | ethernet slot/port | ve
vlan_id ] | neighbor detail | session | statistics ]
```

## Parameters

### igp-sync

Displays the RSVP IGP synchronization information.

#### link

Displays the RSVP IGP synchronization link brief information.

#### detail

Displays the RSVP IGP synchronization link detailed information.

#### ip *ip\_addr*

Displays the RSVP IGP synchronization specified link information.

#### lsp

Displays the RSVP IGP synchronization LSP brief information.

#### detail

Displays the RSVP IGP synchronization LSP detailed information.

#### name *name*

Displays the RSVP IGP synchronization specified LSP information.

#### interface

Displays RSVP interface information.

#### detail

Displays RSVP interface information in detail.

#### ethernet *slot/port*

Displays the specified RSVP Ethernet information.

#### ve *vlan\_id*

Displays the specified VE information.

#### neighbor

Displays the RSVP neighbor information.

#### detail

Displays the RSVP neighbor information in detail.

#### session

Displays the RSVP session information. For additional information, see the **show mpls rsvp session** command page.

#### statistics

Displays the RSVP control packet statistics information.

## Modes

Global configuration mode.

The following example shows the command using the interface option in the interface mode.

```
device(config-if-e1000-1/8)# show mpls interface e1/7
Admin: Up      Oper: Up
MTU: 1500 bytes
Maximum BW: 10000000 kbps, maximum reservable BW: 10000000 kbps
Admin group: 0x00000000
Reservable BW [priority] kbps:
  [0] 10000000   [1] 10000000   [2] 10000000   [3] 10000000
  [4] 10000000   [5] 10000000   [6] 10000000   [7] 10000000
Last sent reservable BW [priority] kbps:
  [0] 10000000   [1] 10000000   [2] 10000000   [3] 10000000
  [4] 10000000   [5] 10000000   [6] 10000000   [7] 10000000
Soft Preemption under provisioned BW [priority] kbps: [0] 0   [1] 0   [2] 0   [3] 0
  [4] 0   [5] 0   [6] 0   [7] 0
LDP tunnel count: 0
```

The following example shows the command using the **interface detail** option in the router mpls mode.

```
device(config-router-mpls)# show mpls rsvp interface detail

Interface State MD5  RelMsg Bundle SRefresh Num of OutSegs Num of
           Up      OFF OFF      OFF      OFF      Act/Inact/Resv Preempts/softPrmpt
e1/1      Up      OFF OFF      OFF      OFF      1/0/1           2/2
e1/2      Up      OFF OFF      OFF      OFF      0/0/0           0/0
e1/10     Dn      OFF OFF      OFF      OFF      0/0/0           0/0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show mpls rsvp interface

Displays the RSVP refresh reduction settings for an interface.

## Syntax

```
show mpls rsvp interface [ detail | [ethernet slot/port] | [ ve vlan_id ] ]
```

## Parameters

### detail

Displays the RSVP interface information in detail.

### ethernet slot/port

Specifies the selected Ethernet interface.

### ve vlan\_id

Specifies the selected VE interface.

## Modes

Privileged EXEC mode.

## Usage Guidelines

To clear the RSVP statistics counters, use the **clear mpls rsvp statistics** command.

This command operates in all modes.

## Command Output

The **show mpls rsvp interface detail** command displays the following information:

Output field	Description
Status	Whether the interface is UP or DOWN.
MD5	Whether RSVP message authentication is enabled on the interface.
RelMsg	Whether RSVP reliable messaging is enabled on the interface.
Bundle	Whether RSVP bundle messages are enabled on the interface.
SRefresh	Whether RSVP summary refresh is enabled on the interface.
<b>MPLS TE flooding thresholds in use</b>	
Hello-interval	The interval between successive hello packets in milliseconds.
Hello-tolerance	The number of hello intervals before the node treats the neighbor as if communication has been lost.
<b>PacketType</b>	
Path	The number of Path messages received with a packet processing error.
Resv	The number of RESV messages received with a packet processing error.
PathErr	The number of PathErr messages received with a packet processing error.

Output field	Description
ResvErr	The number of ResvErr messages received with a packet processing error.
PathTear	The number of PathTear messages received with a packet processing error.
ResvTear	The number of reservation confirmation messages received with a packet processing error.
ResvConf	The number of reservation confirmation messages received with a packet processing error.
Bundle	The number of bundled RSVP messages sent and received on the interface with a packet processing error.
Ack	The number of Ack messages sent and received on the interface with a packet processing error.
SumRefresh	The number of summary refresh messages sent and received on the interface with a packet processing error.
Hello	The number of RSVP Hello's with a packet processing error
<b>Errors</b>	
Rev MD5 Auth Errors	The number of MD5 authentication errors on received packets on the interface.
Pkt with MsgId drop	Number of packets with dropped message IDs.
Pkt with SRef drop	Number of packets with dropped.
NACK Object	Number of objects without acknowledgment.
Active Facility Backups	Number of Active facility backup tunnels.
Inactive Facility Backups	Number of inactive facility backup tunnels.
Duplicate preempts dropped	Number of dropped preempts.

## Examples

The following example shows a abbreviated output of the command with the **detail** option.

```

device# show mpls rsvp interface
G = Interface is using global config for Refresh Reduction, Reliable Messaging
L = Interface is using local config for Refresh Reduction, Reliable Messaging
D = Refresh Reduction, Reliable Messaging is exclusively disabled on Interface

Interface      State   MD5   RelMes   Bundle   SRefresh   Num of OutSeg   Num of
Ve20           Down   OFF   ON<G>    OFF      ON<G>      Act/Inact/Resev Preempts/softPrpt
                                0/0/0          0/0

MPLS TE flooding thresholds in use
  Default      UP   thresholds: 15 30 45 60 75 80 85 90 95 96 97 98 99 100
  Default      DOWN thresholds: 99 98 97 96 95 90 85 80 75 60 45 30 15

Hello-interval: 0 sec, Hello-tolerance: 0 <Hello Inactive, Global configuration>

PacketType     Sent      Total      Received      Since Last Clear
Path           29373     32824      29373         32824
Resv           33047     30209      33047         30209
PathErr        12         0           12            0
ResvErr        89         10          89            10
PathTear       111        45          111           45
ResvTear       0          0           0             0
ResvConf       0          0           0             0
Bundle         0          0           0             0
Ack            0          0           0             0
SumRefresh     0          0           0             0
Hello          0          0           0             0

Errors          Total      Since Last Clear
Rev MD5 Auth Errors 0          0
Pkt with MsgId drop 0          0
Pkt with SRef drop  0          0
NACK Object         0          0

Active Facility Backups: 0
Inactive Facility Backups: 0
Duplicate preempts dropped: 0
....

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show mpls statistics

Displays MPLS statistics.

## Syntax

```
show mpls statistics { oam }
```

```
show mpls statistics { transit [ label label | ldp [ ip_addr | submask | label ] | rsvp label ] }
```

```
show mpls statistics { tunnel [ destination ip_addr | index vif_index | ldp [ destination ip_addr | index vif_index ] | rsvp [ destination ip_addr | index vif_index | name name ] ] }
```

## Parameters

### oam

Displays the MPLS OAM statistics.

### transit

Displays the MPLS transit statistics.

#### label *label*

Displays the MPLS transit statistics for the selected label.

#### ldp *ip\_addr*

Displays the MPLS transit LDP statistics for the selected IP address.

#### rsvp

Displays the MPLS transit RSVP statistics .

### tunnel

Displays the MPLS tunnel statistics.

#### destination *destination*

Displays the MPLS tunnel statistics for the selected tunnel destination.

#### index *vif\_index*

Displays the MPLS tunnel statistics for the selected tunnel index.

#### ldp

Displays the MPLS tunnel LDP statistics.

##### destination *destination*

Displays the MPLS tunnel statistics for the selected tunnel destination.

##### index *vif\_index*

Displays the MPLS tunnel statistics for the selected tunnel index.

#### rsvp

Displays the MPLS tunnel RSVP statistics.

##### destination *destination*

Displays the MPLS tunnel statistics for the selected tunnel destination.

##### index *vif\_index*

Displays the MPLS tunnel statistics for the selected tunnel index.



**name** *name*

Displays the MPLS tunnel statistics for the selected named tunnel.

## Modes

Router MPLS LSP configuration mode.

## Command Output

The **show mpls statistics** command displays the following information:

Output field	Description
Name	Tunnel name.
Intf	Interface tunnel name.
Prot	Protection code: L-Local, R- RtrId
Total Packets	Displays the total number of packets.
Total Bytes	Displays the total number of bytes.
Since Last Clear Packets	Displays the number of packets since last clear.
Since Last Clear Bytes	Displays the number of bytes since the last clear.
Rate Pkts/sec	Displays the packets per second rate.
Rate Bytes/sec	Displays the bytes per second rate.

## Examples

The following example shows the command using the **tunnel** option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics tunnel
```

Name	Intf	Prot	Total		Since Last clear		Pkts/sec	Rate Bytes/sec
			Packets	Bytes	Packets	Bytes		
t1	tn10	R	2004	28175882	2004	28175882	6	93919
t2	tn11	L	3101	40373763	3101	40373763	10	134579

The following example shows the command using the **tunnel rsvp** option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics tunnel rsvp
```

Name	Intf	Total		Since Last clear		Pkts/sec	Rate Bytes/sec
		Packets	Bytes	Packets	Bytes		
t1	tn10	2004	28175882	2004	28175882	6	93919

The following example shows the command using the **transit** option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics transit
```

IN Label	Prot	Total		Since Last clear		Pkts/sec	Rate Bytes/sec
		Packets	Bytes	Packets	Bytes		
2048	R	2004	28175882	2004	28175882	6	93919
2050	L	3101	40373763	3101	40373763	10	134579

The following example shows the command using the **transit ldp** option.

```

device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics transit ldp

```

IN Label	Total		Since Last clear		Pkts/sec	Rate
	Packets	Bytes	Packets	Bytes		Bytes/sec
2050	3101	40373763	3101	40373763	10	134579

## History

Release version	Command history
16r.1.01	This command was introduced.

# show mpls te database

Fate-sharing group membership for any given TE link or node consists of its own membership to the group, and the TE node to which it belongs. The output from the **show mpls te database detail** command displays the fate-sharing groups to which the TE links or nodes belong.

## Syntax

```
show mpls te [ area ipv4_addr | detail | link ipv4_addr | node ipv4_addr ]
```

## Parameters

**area** *ipv4\_addr*

Displays the specified OSPF area or ISIS level information.

**detail**

Displays detailed information.

**link***ipv4\_addr*

Displays the specified link information.

**node***ipv4\_addr*

Displays the specified node information by the node router ID.

## Modes

EXEC mode.

## Examples

In the following example output, node *10.20.20.20* displays fate-sharing group information for *group1/100* and *group2/10*.

```
device# show mpls te database detail
This Router is 10.100.100.100
Global Link Gen 21
Area 0
NodeID: 10.20.20.20, Type: Router
info from applied local policies:
  cspf-group member information (name/penalty):
    group1/100
    Type: P2P, To: 10.1.1.1, Local: 10.1.1.2, Remote: 10.1.1.1, Gen 16
    Admin Group: 0x00000000
    Metric: 1
    Link BW: 10000000 kbits/sec
    Reservable BW: 10000000 kbits/sec
    Unreserved BW:
      [0] 10000000 kbits/sec [1] 10000000 kbits/sec
      [2] 10000000 kbits/sec [3] 10000000 kbits/sec
      [4] 10000000 kbits/sec [5] 10000000 kbits/sec
      [6] 10000000 kbits/sec [7] 10000000 kbits/sec
info from applied local policies:
  cspf-group member information (name/penalty):
    group2/10
    Type: P2P, To: 10.1.2.1, Local: 10.1.2.2, Remote: 10.1.2.1, Gen 13
    Admin Group: 0x00000000
    Metric: 1
    Link BW: 10000000 kbits/sec
    Reservable BW: 10000000 kbits/sec
    Unreserved BW:
      [0] 10000000 kbits/sec [1] 10000000 kbits/sec
      [2] 10000000 kbits/sec [3] 10000000 kbits/sec
      [4] 10000000 kbits/sec [5] 10000000 kbits/sec
      [6] 10000000 kbits/sec [7] 10000000 kbits/sec
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show openflow

Displays the OpenFlow configuration at the global level.

## Syntax

```
show openflow
```

## Modes

Privileged EXEC mode

## Usage Guidelines

It includes the asynchronous messages sent to the controller.

## Examples

```

device# show openflow
Administrative Status:      Enabled
SSL Status:                 Enabled
Datapath-ID:               8ff88e740000
Number of Controllers:     3

Controller:                 A1
Controller Type:           OFV130
Connection Mode:          active TCP
Listening Address:        10.24.5.5
Connection Port:          1987
VRF Name:                 mgmt-vrf
Source IP used:           NA
Connection Status:        CLOSE
Role:                     Equal
  Asynchronous Configuration: Packet-in (no-match|action)
                             Port-status (add|delete|modify)
                             Flow-removed (idle-timeout|hard-timeout|delete|grp-delete)

Controller:                 A2
Controller Type:           OFV130
Connection Mode:          active SSL
Listening Address:        10.24.5.5
Connection Port:          1987
VRF Name:                 mgmt-vrf
Source IP used:           NA
Connection Status:        TCP_CONNECTING
Role:                     Equal
  Asynchronous Configuration: Packet-in (no-match|action)
                             Port-status (add|delete|modify)
                             Flow-removed (idle-timeout|hard-timeout|delete|grp-delete)

Controller:                 A3
Controller Type:           OFV130
Connection Mode:          active TCP
Listening Address:        10.24.5.5
Connection Port:          1987
VRF Name:                 mgmt-vrf
Source IP used:           NA
Connection Status:        CLOSE
Role:                     Equal
  Asynchronous Configuration: Packet-in (no-match|action)
                             Port-status (add|delete|modify)
                             Flow-removed (idle-timeout|hard-timeout|delete|grp-delete)

Connection Status:        OPENFLOW_ESABLISHED
Role:                     Equal
  Asynchronous Configuration: Packet-in (no-match|action)
                             Port-status (add|delete|modify)
                             Flow-removed (hard-timeout|delete|grp-delete)

Match Capability:
L2 : Port, Source MAC, Destination MAC, Ether type, Vlan, Vlan PCP
L3 : Port, Vlan, vlan PCP, Ethertype, Source IP, Destination IP, IP Protocol, IP TOS,TCP/UDP Src Port,
TCP/UDP Dst Port
L23: All

Openflow Enabled Ports: Eth 3/25, Eth 3/26

Default action: DROP
Maximum number of flows allowed: 32768
Active flow: 0

device#

```

TABLE 2 Output fields for the show openflow command

Field	Description
Administrative Status	Indicates the administrative status of OpenFlow on the device.
SSL status	Indicates the SSL status of OpenFlow controller on the device.
Data path ID	Displays the data path ID assigned to the device.
Number of Controllers	Lists the number of controller connections configured on the device.
Controller Type	Indicates the OpenFlow protocol version that is supported on the device.
Connection mode	Indicates the mode of the controller connection configured. You can configure active or passive connection to controllers. An active connection is initiated by the device. In a passive connection, the device is in the listening mode, and accepts requests from controllers. If the optional controller address is not specified, any controller can establish a connection with the device in the passive mode. If there is an address, only that IP address can connect to the device in passive mode.
Connection port	Indicates the TCP port that is used for connection to the controller. By default, port 6633 is used.
Connection status	Indicates the status of the specified controller.
Role	Indicates the role of the specified controller.
Asynchronous configuration	Asynchronous messages sent to the specified controller.
Match capability	Specifies the matching rules supported for Layer 2 and Layer 3.
OpenFlow enabled ports	Lists the ports on the device that are enabled for OpenFlow.
Default action	Indicates the default action for packets that do not match any configured flows. By default, such packets are dropped. However, you can configure these packets to be sent to the controller by using the <b>default-behavior send-to-controller</b> command.
Maximum number of flows allowed	Indicates the maximum number of flows allowed on the device that is configured by using the <b>system-max openflow-flow-entries</b> command.

## History

Release version	Command history
16r.1.00	This command was introduced.

# show openflow controller

Displays the status of the OpenFlow controller.

## Syntax

`show openflow controller`

## Modes

Privileged EXEC mode

## Examples

The following example displays the status of the OpenFlow controller.

```
device# show openflow controller
Controller Mode  TCP/SSL IP-address  Port  Status      Role
A1      active  TCP      10.24.5.5  1987  CLOSE       Equal
A2      active  SSL      10.24.5.5  6633  TCP_CONNECTING Equal
A3      active  TCP      10.24.5.5  6653  CLOSE       Equal
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show openflow flow

Displays the OpenFlow flow that are configured on the devices with IPv4 fields at the global level.

## Syntax

```
show openflow flow
```

## Modes

Privileged EXEC mode

## Examples

The **show openflow flow** command has the match capability as below.

Layer 2: Port, Source MAC, Destination MAC, Ether type, VLAN, VLAN PCP

Layer 3 : Port, VLAN, VLAN PCP, Ethertype, Source IP, Destination IP, IP Protocol, IP ToS , IP Source Port, IP Destination Port

```
device # show openflow flow
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 Generic based Flows: 0

Total Number of Openflow interfaces:  4
    Total Number of L2 interfaces:  0
    Total Number of L3 interfaces:  1
    Total Number of L23 interfaces:  2

Flow ID: 1 Priority: 32768 Status: Programmed
Rule:
    In Port:                Eth 3/25
    In Vlan:                Tagged[100]
    Vlan Priority:          5
    Source Mac:            0000.0011.1111
    Destination Mac:      0000.0011.1111
    Ether type:            0x800
    Source IPv4:           1.1.1.0
    Source IPv4 Mask:     255.255.255.0
    IP DSCP:                6

Instructions: Apply-Actions
    Action: FORWARD
                Out Port: Eth 3/26, Push-vlan-tag: 0x8100, vlanid: 232
                Vlan Priority: 5

Statistics:
    Total Pkts:  0
    Total Bytes: 0
```

**TABLE 3** Output fields for the show openflow flow command

Field	Description
Total Number of Flows	The total number of flows on the device.
Total number of data packets sent to controller	The number of packets sent to the controller.
Total number of data bytes sent to controller	The number of bytes sent to the controller.

**TABLE 3** Output fields for the show openflow flow command (continued)

Field	Description
Priority	The priority of the flow set by the controller when the flow is added, in the range 0 to 65536. If the priority value was not specified, the device will assign the default value, 32768.
Status	Indicates whether the flow is configured correctly in the device. A correctly configured flow will have its status as active.
Rule	Specifies the matching rule for the flow.
Instruction	Applies the specified actions immediately.
Statistics	Indicates the counter of packets and bytes.

## History

Release version	Command history
16r.1.00	This command was introduced.

# show openflow group

Displays all the groups in a flow for an OpenFlow port.

## Syntax

```
show openflow group
```

## Modes

Privileged EXEC mode

## Usage Guidelines

The hardware resources are shared between OpenFlow and other features, so these resources are allocated on a first-come-first-serve basis.

## Examples

The command displays the minimum and maximum traffic rates for each ports.

```
device# show openflow group
Max number of total groups          : 512
Max number of buckets per group    : 8

TOTAL number of groups(Type:ALL) in the system      : 1
TOTAL number of groups(Type:SELECT) in the system  : 0
TOTAL number of groups(Type:Indirect)in the system : 0
TOTAL number of groups(Type:Fast Failover)in the system : 0

TOTAL number of groups in the system                : 1

Group id 1
Transaction id          4043243760 (f0ff00f0)
Type                   ALL
Packet Count           0
Byte Count             0
Flow Count             0
Number of buckets      2
bucket # 1
  Weight                1
  out port: Eth 3/25,
bucket # 2
  Weight                1
  out port: Eth 3/26,
```

**TABLE 4** Output fields for the show openflow group command

Field	Description
Total number of groups	Total number of group of all types available on the flow, e.g. All, Indirect and Select.
Group ID	Displays the group ID number.
Transaction ID	Unique transaction ID for the specified group ID.
Type	Group type.
Packet count	The number of packets sent in the group.

**TABLE 4** Output fields for the show openflow group command (continued)

Field	Description
Byte count	The number of bytes in the group.
Flow count	The number of flow in the group.
Number of buckets	Number of buckets per group.

## History

Release version	Command history
16r.1.00	This command was introduced.

# show openflow interface

Displays the detailed interface configuration and capabilities of all interfaces.

## Syntax

```
show openflow interface
```

## Modes

Privileged EXEC mode

## Examples

To show OpenFlow interface, enter the following command:

```
device # show openflow interface
Total number of Openflow interfaces: 4
Port    Link    Port-State  Speed    MAC                OF-Port-ID  Mode
Eth 3/25 Up      Forward    40G 748e.f88f.e9c7  868         123
Eth 3/26 Down    Forward    40G 748e.f88f.e9c8  872         123
Eth 3/27 Down    Forward    40G 748e.f88f.e9c9  876         13
Eth 3/28 Down    Forward    40G 748e.f88f.e9ca  880         hybrid 123
```

**TABLE 5** Output fields of the show openflow interface command

Field	Description
Port	Indicates the port number on the device.
Link	Indicates the link status.
Port-State	Indicates the action to be performed on packets that reach the interface.
Speed	Indicates the port speed.
MAC	Indicates the MAC address of the port.
OF-Port-ID	Indicates the OpenFlow port ID that is assigned to the port on the device. Port numbers on the device are mapped to OpenFlow port IDs.
Mode	Indicates the OpenFlow mode enabled on the port.

## History

Release version	Command history
16r.1.00	This command was introduced.

# show openflow meter

Displays all the meters in a flow for an OpenFlow port.

## Syntax

```
show openflow meter
```

## Modes

Privileged EXEC mode

## Usage Guidelines

The hardware resources are shared between OpenFlow and other features, so these resources are allocated on a first-come,-first-served basis.

## Examples

```
Device# show openflow meter
TOTAL Meters: 1
Meter id: 1
  Transaction id:      4043243760
  Meter Flags:        KBPS BURST
  Flow Count:         0
  Number of bands:    1
  In packet count:    NA
  In byte count:      0
  Band Type:          DROP
    Rate:              30 kbps
    Burst size:         10000 kbps
  In packet band count: NA
  In byte band count: 0
device#
```

**TABLE 6** Output fields for the show openflow meter command

Field	Description
Total number of meters	Total number of meters available in the flow.
Meter ID	Displays the meter ID number.
Transaction ID	Unique transaction ID for the specified meter ID.
Meter flags	Metering capability.
Flow count	The number of flow in the meter.
Number of bands	Number of bands per meter.
Band type	Band type supported on the meter. Supported band type is DROP.

## History

Release version	Command history
16r.1.00	This command was introduced.

# show openflow queues

Displays the queue entries for an interface for an OpenFlow port.

## Syntax

```
show openflow queues
```

## Modes

Privileged EXEC mode

## Usage Guidelines

Ensure that OpenFlow queuing is configured on the device. You can associate a flow with an `OFFPAT_ENQUEUE` action which forwards the packet through the specific queue on a port.

## Examples

The command displays the minimum and maximum traffic rates for each ports.

```
device# show openflow queues
Openflow Port      Eth 3/26
Queue 0
  Tx Packets: 0
  Tx Bytes: : 0
Queue 1
  Tx Packets: 0
  Tx Bytes: : 0
Queue 2
  Tx Packets: 0
  Tx Bytes: : 0
Queue 3
  Tx Packets: 0
  Tx Bytes: : 0
Queue 4
  Tx Packets: 0
  Tx Bytes: : 0
Queue 5
  Tx Packets: 0
  Tx Bytes: : 0
Queue 6
  Tx Packets: 0
  Tx Bytes: : 0
Queue 7
  Tx Packets: 0
  Tx Bytes: : 0
```

**TABLE 7** Output fields for the show openflow queues command

Field	Description
OpenFlow port	Slot and port number.
Queue	Displays the queue number for the specified OpenFlow port.
Packet	The number of transmitted packets in the queue.
Byte	The number of transmitted bytes in the queue.

## History

Release version	Command history
16r.1.00	This command was introduced.



# show openflow resources

Displays the OpenFlow usage of the resources at the global level.

## Syntax

show openflow resources

## Modes

Privileged EXEC mode

## Examples

```
device# show openflow resources
Used - Number of HW entries consumed
Free - Number of Port based flows that can be successfully Slot: 1 Module: slot 1
Openflow Flows: MAX: 8192      Used: 0      Free: 819
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Slot: 2      Module: slot 2
Openflow Flows: MAX: 8192      Used: 0      Free: 819
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Slot: 3      Module: slot 3
Openflow Flows: MAX: 8192      Used: 1      Free: 819
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 1      Free: 4095
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Slot: 4      Module: slot 4
Openflow Flows: MAX: 8192      Used: 0      Free: 819
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Chip Flows: MAX: 4096      Used: 0      Free: 4096
Openflow Meter Resources: MAX: 1023
Used: 1
ALL MAX: 512      Used: 1      Free: 511
Tcam Profile:      Openflow Optimized 2
```

TABLE 8 Output fields for the show openflow resources command

Field	Description
Used	Number of hardware entries.
Free	Number of port based flows, that can be programmed.
Slot	Indicates the slot number
Module	Indicates the device number

**TABLE 8** Output fields for the show openflow resources command (continued)

Field	Description
OpenFlow flows	Available, used and maximum number of OpenFlow flows for Layer 2 and Layer 3.
OpenFlow Meter resources	Available, used and maximum number of OpenFlow meters for the device.

## History

Release version	Command history
16r.1.00	This command was introduced.

# show policy-map

Displays configured policy-maps and class-map Policer parameters applied to switch interfaces.

## Syntax

```
show policy-map [ details polycyname | interface ethernet slot/port [ input | output ] ]
```

## Parameters

**details** *polycyname*

Displays the detail configuration of the policy-map along with binding information.

**interface ethernet**

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

*slot/port*

Specifies a valid slot and port number.

**input** |

Inbound - direction where the policy map is applied.

**output**

Outbound - direction where the policy map is applied.

## Modes

Global configuration mode

Interface configuration mode

## Usage Guidelines

Use this command with a specific interface to display the policy map binding settings (policy map name and traffic direction), police-priority-map applied, and class map policer parameters applied for that interface.

Use this command without identifying an interface and direction of traffic to display policy map binding for all interfaces on the switch.

## Command Output

The **show policy-map** command displays the following information:

Output field	Description
Interface	The interface for which rate limiting information is being displayed.
Direction	The traffic direction for which rate limiting is applied.
police-priority-map	Remarkd priority map used for Policer application (802.1 p priority remarked map).
Conform	The traffic in bytes that has been forwarded from this interface that is within the CIR bandwidth limits.

Output field	Description
Exceeded	The traffic that has been exceeded the bandwidth available in the CIR limits and has not exceed the EIR limits for this rate-limit policy.
Violated	The traffic that has exceeded the bandwidth available in the CIR and EIR limits.
set-dscp	The DSCP value which is applied to the traffic for the given color (conform, exceed, violate).
set-tc	The remapped traffic class queue for the traffic for the given color (conform, exceed, violate).
Total	The total traffic in bytes carried on this interface for the defined rate-limit policy.

## Examples

To display policy-map binding and class map parameters applied to a specific interface:

```
device# show policy-map interface ethernet 4/1 input
Interface : Ethernet 4/1
policy-map: policy-mapA-1
Direction: Input
Input Excluded lossless priorities: None

Class-map: default
  Police:
    cir 5 bps cbs 5678 bytes eir 512000 bps ebs 4096 bytes
    Police-priority-map: po-pr-map1
    Conformed: 30720 bytes set-dscp 0 set-tc 0
    Exceeded: 23424 bytes set-dscp 0 set-tc 0
    Violated: 0 bytes
    Total: 54144 bytes
```

To display policy map binding information for all interfaces:

```
device# show policy-map
Interface : Ethernet 4/2
Inbound policy map is policy-mapA-1
Outbound policy map is not set
Interface : Ethernet 4/3
Inbound policy map is not set
Outbound policy map is not set
Interface : Ethernet 4/4
Inbound policy map is not set
Outbound policy map is not set
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show port-security

Displays the configuration information related to port security.

## Syntax

```
show port-security [ addresses | interface ethernet slot/port ]
```

## Modes

Privileged EXEC mode

Interface configuration mode

## Command Output

The **show port-security** command displays the following information:

Output field	Description
Secure Port	The port on which port MAC security is enabled.
MaxSecureAddress (count)	The maximum limit for the number of secure MAC addresses allowed on the interface.
StaticSec (count)	The number of MAC addresses that are manually configured.
Violated	The status that shows whether the port security violation has occurred.
Action	The configured response action that will be taken when a port security violation occurs.
Sticky	The status that shows whether sticky MAC learning is enabled.
Port Security	The status that shows whether port MAC security is enabled.
Port Status	The status of the port.
Violation Mode	The configured response action that will be taken when a port security violation occurs.
Violated	The status that shows whether the port security violation has occurred.
Sticky Enabled	The status that shows whether sticky MAC learning is enabled.
Maximum MAC addresses	The maximum limit for the number of secure MAC addresses allowed on the interface.
Total MAC addresses	The total number of secure MAC addresses learned on the interface.
Configured MAC addresses	The total number of secure MAC addresses configured on the interface manually.
Last violation time	The time when the last port security violation occurred.
Shutdown time (in Minutes)	The configured auto recovery time for port security violation.
Vlan	The VLAN to which the port is mapped.
Mac-address	The secured MAC address.
Type	The types of secure MAC addresses that are used in port MAC security.
Ports	The port on which port MAC security is enabled.

## Examples

To display the port MAC security configuration details across ports on the device, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security
Secure      MaxSecureAddr  CurrentAddr  StaticSec  Violated  Action  Sticky
Port        (count)        (count)      (count)
Eth 3/2     10             0            1          No        Shutdown No
```

To display the statistics of the port MAC security configured for an interface, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security interface ethernet 3/2
Port Security           : Enabled
Port Status             : Up
Violation Mode          : Shutdown
Violated                 : No
Sticky Enabled          : No
Maximum MAC addresses   : 10
Total MAC addresses     : 0
Configured MAC addresses : 1
Last violation time     :
Shutdown time (in Minutes) : 0
```

To list the secure MAC addresses configured on the device, enter the following command.

```
device(conf-if-eth-3/2)# do show port-security addresses
Secure Mac Address Table
-----
Vlan      Mac-address      Type              Ports
250       3200.1110.0002  Secure-Static    Eth 3/2
```

# show qos cpu cfg

Displays information about the current CPU protection configuration for individual slots.

## Syntax

```
show qos cpu cfg { slotslot_id } [ burst | shaper | rate ]
```

## Parameters

### *slotslot\_id*

Specifies a slot number. The ranges are 0 on pizzabox platforms, 1 through 4 on F4 platforms, and 1 through 8 on F8 platforms.

### burst

Specifies port and group traffic burst rates for IPv6 subnet rate limiting.

### shaper

Specifies port and group traffic shaper rates for IPv6 subnet rate limiting.

### rate

Specifies shaping rate for IPv6 subnet rate limiting.

## Modes

Privileged EXEC mode

## Usage Guidelines

ipv6 subnet-rate-limit

## Examples

To display information about the CPU configuration for slot 1.

```
device# show qos cpu cfg slot 1
Slot 1 CPU QoS Config
```

CPU Port shaper rate: 5000 Kbps

CPU Group shaper rates (Kbps)

Group	Aggr	P0	P1	P2	P3	P4	P5	P6	P7
0	5000	5000	5000	5000	5000	5000	5000	5000	5000
1	5000	5000	5000	5000	5000	5000	5000	5000	5000
2	5000	5000	5000	5000	5000	5000	5000	5000	5000
3	5000	5000	5000	5000	5000	5000	5000	5000	5000
4	5000	5000	5000	5000	5000	5000	5000	5000	5000
5	5000	5000	5000	5000	5000	5000	5000	5000	5000
6	5000	5000	5000	5000	5000	5000	5000	5000	5000
7	5000	5000	5000	5000	5000	5000	5000	5000	5000
8	5000	5000	5000	5000	5000	5000	5000	5000	5000
9	5000	5000	5000	5000	5000	5000	5000	5000	5000
10	5000	5000	5000	5000	5000	5000	5000	5000	5000
11	5000	5000	5000	5000	5000	5000	5000	5000	5000

CPU Port burst size: 1 Kbytes

CPU Group burst size (Kbytes)

Group	Aggr	P0	P1	P2	P3	P4	P5	P6	P7
0	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1
4	1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	1	1
8	1	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1

CPU Group WFQ values

Group	Aggr	P0	P1	P2	P3	P4	P5	P6	P7
0	1	20	50	50	50	50	50	50	100
1	1	20	50	50	50	50	50	50	100
2	1	20	50	50	50	50	50	50	100
3	1	20	50	50	50	50	50	50	100
4	1	20	50	50	50	50	50	50	100
5	1	20	50	50	50	50	50	50	100
6	1	20	50	50	50	50	50	50	100
7	1	20	50	50	50	50	50	50	100
8	1	20	50	50	50	50	50	50	100
9	1	20	50	50	50	50	50	50	100
10	1	20	50	50	50	50	50	50	100
11	1	20	50	50	50	50	50	50	100



To display information only about the IPv6 subnet rate-limiting traffic shaper configuration for slot 1.

```
device# show qos cpu cfg slot 1 shaper
Slot 1 CPU QoS Config
```

```
CPU Port shaper rate: 5000 Kbps
```

```
CPU Group shaper rates (Kbps)
```

Group	Aggr	P0	P1	P2	P3	P4	P5	P6	P7
0	5000	5000	5000	5000	5000	5000	5000	5000	5000
1	5000	5000	5000	5000	5000	5000	5000	5000	5000
2	5000	5000	5000	5000	5000	5000	5000	5000	5000
3	5000	5000	5000	5000	5000	5000	5000	5000	5000
4	5000	5000	5000	5000	5000	5000	5000	5000	5000
5	5000	5000	5000	5000	5000	5000	5000	5000	5000
6	5000	5000	5000	5000	5000	5000	5000	5000	5000
7	5000	5000	5000	5000	5000	5000	5000	5000	5000
8	5000	5000	5000	5000	5000	5000	5000	5000	5000
9	5000	5000	5000	5000	5000	5000	5000	5000	5000
10	5000	5000	5000	5000	5000	5000	5000	5000	5000
11	5000	5000	5000	5000	5000	5000	5000	5000	5000

To display information only about the IPv6 subnet shaping rate configuration for slot 1.

```
device# show qos cpu cfg slot 1 rate
Slot 1 CPU QoS Config
```

Name	Egid	Group	Pkts	Bytes	PPS	bps
Protocol	7f80	0	0	0	0	0
Management	7f81	1				
IP Host	7f82	2	11907	173855778	724	845632
MC RPF Fail	7f83	3	0	0	0	0
MC LHR	7f84	4	0	0	0	0

## History

Release version	Command history
16r.1.01	This command was modified to support IPv6 subnet rate limiting.

# show qos cpu info

Displays information on CPU groups and effective group IDs (EGID).

## Syntax

```
show qos cpu info
```

## Modes

Privileged EXEC mode.

## Examples

To show CPU group information use the following command.

```
device# show qos cpu info
```

Name	Egid	Group	Description
Protocol	7f80	0	Protocol Packets (ARP, L2, etc)
Management	7f81	1	Management (ping, local route)
IP Host	7f82	2	IP Host (subnet route)
MC RPF Fail	7f83	3	Multicast RPF failure
MC LHR	7f84	4	Multicast RP and LHR
MC FHR	7f85	5	Multicast FHR
SFlow Port	7f86	6	SFlow Packets (Port sflow)
SFlow ACL In	7f87	6	ACL sflow ingress permit
SFlow ACL In Deny	7f88	6	ACL sFlow ingress deny
SFlow ACL Eg	7f89	6	ACL sflow egress permit
SFlow ACL Eg Deny	7f8a	6	ACL sflow egress deny
VXLAN Snoop	7f8b	6	VXLAN Visibility Snoop
ACL Log	7f8c	7	ACL Logging
ACL Log In	7f8d	7	ACL Logging ingress permit
ACL Log In Deny	7f8e	7	ACL Logging ingress deny
ACL Log Eg	7f8f	7	ACL Logging egress permit
ACL Log Eg Deny	7f90	7	ACL Logging egress deny
Snoop	7f91	8	Snoop (VxLAN)
Diagnostics	7f92	9	Diagnostics and debug
OAM	7f93	10	OAM and CFM
Openflow	7f94	11	OpenFlow packets
Exceptions	7f96	12	Errors, Exceptions (TTL, MTU)
ICMP Redirect	7f95	12	ICMP Redirect

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos interface all

Displays QoS configuration information about Ethernet, Virtual Ethernet, and port-channel interfaces.

## Syntax

```
show qos interface all
```

## Modes

Privileged EXEC mode.

## Usage Guidelines

## Examples

To show QoS information for all interfaces use the following command.

```

device show qos interface all
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ve 20
  Provisioning Mode: none

  DSCP Mutation Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 01 02 03 04 05 06 07 08 09
    1 : 10 11 12 13 14 15 16 17 18 19
    2 : 20 21 22 23 24 25 26 27 28 29
    3 : 30 31 32 33 34 35 36 37 38 39
    4 : 40 41 42 43 44 45 46 47 48 49
    5 : 50 51 52 53 54 55 56 57 58 59
    6 : 60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
    1 : 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0 2/0
    2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
    3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
    4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
    5 : 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0 7/0
    6 : 7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 00 00 00 00 00 00 00 00 01 01
    1 : 01 01 01 01 01 01 02 02 02 02 02
    2 : 02 02 02 02 03 03 03 03 03 03 03
    3 : 03 03 04 04 04 04 04 04 04 04 04
    4 : 05 05 05 05 05 05 05 05 05 06 06
    5 : 06 06 06 06 06 06 07 07 07 07 07
    6 : 07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
    TC: 0 1 2 3 4 5 6 7
    -----
  Threshold: 0 0 0 0 0 0 0 0

  Flow control mode Off

  ...

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 2/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
    In-CoS: 0 1 2 3 4 5 6 7
    -----
    Out-TC: 0 1 2 3 4 5 6 7
    Out-DP: 0 0 0 0 0 0 0 0

  TC-to-CoS Map: default
    In-TC: 0 1 2 3 4 5 6 7
    -----

```

```

Out-CoS (DP=0): 0 1 2 3 4 5 6 7
Out-CoS (DP=1): 0 1 2 3 4 5 6 7
Out-CoS (DP=2): 0 1 2 3 4 5 6 7
Out-CoS (DP=3): 0 1 2 3 4 5 6 7

DSCP Mutation Map: default (DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63

DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
1 : 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0 2/0
2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 : 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0 7/0
6 : 7/0 7/0 7/0 7/0 7/0 7/0 7/0 7/0 7/0 7/0 7/0

DSCP-to-CoS Map: default (DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 00 01 01
1 : 01 01 01 01 01 01 02 02 02 02 02
2 : 02 02 02 02 03 03 03 03 03 03 03
3 : 03 03 04 04 04 04 04 04 04 04 04
4 : 05 05 05 05 05 05 05 05 05 06 06
5 : 06 06 06 06 06 06 07 07 07 07 07
6 : 07 07 07 07 07 07 07 07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)
TC: 0 1 2 3 4 5 6 7
-----
Threshold: 0 0 0 0 0 0 0 0

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/125
Provisioning Mode: none
Default TC: 0

CoS-to-TC Map: default
In-CoS: 0 1 2 3 4 5 6 7
-----
Out-TC: 0 1 2 3 4 5 6 7
Out-DP: 0 0 0 0 0 0 0 0

TC-to-CoS Map: default
In-TC: 0 1 2 3 4 5 6 7
-----
Out-CoS (DP=0): 0 1 2 3 4 5 6 7
Out-CoS (DP=1): 0 1 2 3 4 5 6 7
Out-CoS (DP=2): 0 1 2 3 4 5 6 7
Out-CoS (DP=3): 0 1 2 3 4 5 6 7

DSCP Mutation Map: default (DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39

```

show qos interface all

```
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
```

DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)

```
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
1 : 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0 2/0
2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 : 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0 7/0
6 : 7/0 7/0 7/0 7/0
```

DSCP-to-CoS Map: default (DSCP = d1d2)

```
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 01 01
1 : 01 01 01 01 01 01 02 02 02 02
2 : 02 02 02 02 03 03 03 03 03 03
3 : 03 03 04 04 04 04 04 04 04 04
4 : 05 05 05 05 05 05 05 05 06 06
5 : 06 06 06 06 06 06 07 07 07 07
6 : 07 07 07 07
```

Per Traffic-Class Tail Drop Threshold (bytes)

```
TC: 0 1 2 3 4 5 6 7
-----
Threshold: 0 0 0 0 0 0 0 0
```

Flow control mode Off

... <output truncated>

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos interface ethernet

Displays QoS configuration information for a specific Ethernet interface.

## Syntax

```
show qos interface ethernet } slot/port
```

## Parameters

*slot/port*

A specific Ethernet interface slot and port number.

## Modes

Privileged EXEC mode.

## Examples

To display the QoS configuration for a specific interface use the following command.

```
device# show qos interface ethernet 1/19
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/19
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
    In-CoS: 0 1 2 3 4 5 6 7
    -----
    Out-TC: 0 1 2 3 4 5 6 7
    Out-DP: 0 0 0 0 0 0 0 0

  TC-to-CoS Map: default
    In-TC: 0 1 2 3 4 5 6 7
    -----
    Out-CoS (DP=0): 0 1 2 3 4 5 6 7
    Out-CoS (DP=1): 0 1 2 3 4 5 6 7
    Out-CoS (DP=2): 0 1 2 3 4 5 6 7
    Out-CoS (DP=3): 0 1 2 3 4 5 6 7

  DSCP Mutation Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 01 02 03 04 05 06 07 08 09
    1 : 10 11 12 13 14 15 16 17 18 19
    2 : 20 21 22 23 24 25 26 27 28 29
    3 : 30 31 32 33 34 35 36 37 38 39
    4 : 40 41 42 43 44 45 46 47 48 49
    5 : 50 51 52 53 54 55 56 57 58 59
    6 : 60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
    1 : 1/0 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
    2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
    3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
    4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
    5 : 6/0 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
    6 : 7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 00 00 00 00 00 00 00 01 01
    1 : 01 01 01 01 01 01 02 02 02 02
    2 : 02 02 02 02 03 03 03 03 03 03
    3 : 03 03 04 04 04 04 04 04 04 04
    4 : 05 05 05 05 05 05 05 05 06 06
    5 : 06 06 06 06 06 06 06 07 07 07
    6 : 07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
    TC: 0 1 2 3 4 5 6 7
    -----
  Threshold: 0 0 0 0 0 0 0 0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
```



## History

Release version	Command history
16r.1.00	This command was introduced.

show qos interface port-channel

# show qos interface port-channel

Displays QoS configuration information about a specific port channel interface.

## Syntax

```
show qos interface port-channel port_channel_number
```

## Parameters

*port\_channel\_number*

A specific port channel number.

## Modes

Privileged EXEC mode.

## Usage Guidelines

## Examples

Follow this example to view information about the insight interface port channel on MM 1.

```

device# show qos interface port-channel 1
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 3/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
    In-CoS: 0 1 2 3 4 5 6 7
    -----
    Out-TC: 0 1 2 3 4 5 6 7
    Out-DP: 0 0 0 0 0 0 0 0

  TC-to-CoS Map: default
    In-TC: 0 1 2 3 4 5 6 7
    -----
    Out-CoS (DP=0): 0 1 2 3 4 5 6 7
    Out-CoS (DP=1): 0 1 2 3 4 5 6 7
    Out-CoS (DP=2): 0 1 2 3 4 5 6 7
    Out-CoS (DP=3): 0 1 2 3 4 5 6 7

  DSCP Mutation Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 01 02 03 04 05 06 07 08 09
    1 : 10 11 12 13 14 15 16 17 18 19
    2 : 20 21 22 23 24 25 26 27 28 29
    3 : 30 31 32 33 34 35 36 37 38 39
    4 : 40 41 42 43 44 45 46 47 48 49
    5 : 50 51 52 53 54 55 56 57 58 59
    6 : 60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
    1 : 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0 2/0
    2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
    3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
    4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
    5 : 6/0 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
    6 : 7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 00 00 00 00 00 00 00 01 01
    1 : 01 01 01 01 01 01 02 02 02 02
    2 : 02 02 02 02 03 03 03 03 03 03
    3 : 03 03 04 04 04 04 04 04 04 04
    4 : 05 05 05 05 05 05 05 05 06 06
    5 : 06 06 06 06 06 06 07 07 07 07
    6 : 07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
    TC: 0 1 2 3 4 5 6 7
    -----
  Threshold: 0 0 0 0 0 0 0 0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

```

show qos interface port-channel

```
Interface Ethernet 2/125
Provisioning Mode: none
Default TC: 0

CoS-to-TC Map: default
-----
In-CoS: 0 1 2 3 4 5 6 7
-----
Out-TC: 0 1 2 3 4 5 6 7
Out-DP: 0 0 0 0 0 0 0 0

TC-to-CoS Map: default
-----
In-TC: 0 1 2 3 4 5 6 7
-----
Out-CoS (DP=0): 0 1 2 3 4 5 6 7
Out-CoS (DP=1): 0 1 2 3 4 5 6 7
Out-CoS (DP=2): 0 1 2 3 4 5 6 7
Out-CoS (DP=3): 0 1 2 3 4 5 6 7

DSCP Mutation Map: default (DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63

DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
1 : 1/0 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 : 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0 7/0
6 : 7/0 7/0 7/0 7/0

DSCP-to-CoS Map: default (DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 01 01
1 : 01 01 01 01 01 01 01 02 02 02 02
2 : 02 02 02 02 03 03 03 03 03 03
3 : 03 03 04 04 04 04 04 04 04 04
4 : 05 05 05 05 05 05 05 05 06 06
5 : 06 06 06 06 06 06 07 07 07 07
6 : 07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)
-----
TC: 0 1 2 3 4 5 6 7
-----
Threshold: 0 0 0 0 0 0 0 0

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/125
Provisioning Mode: none
Default TC: 0

CoS-to-TC Map: default
-----
In-CoS: 0 1 2 3 4 5 6 7
-----
Out-TC: 0 1 2 3 4 5 6 7
Out-DP: 0 0 0 0 0 0 0 0

TC-to-CoS Map: default
-----
In-TC: 0 1 2 3 4 5 6 7
```

```

-----
Out-CoS (DP=0): 0 1 2 3 4 5 6 7
Out-CoS (DP=1): 0 1 2 3 4 5 6 7
Out-CoS (DP=2): 0 1 2 3 4 5 6 7
Out-CoS (DP=3): 0 1 2 3 4 5 6 7

DSCP Mutation Map: default (DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63

DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
1 : 1/0 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0
2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 : 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
6 : 7/0 7/0 7/0 7/0

DSCP-to-CoS Map: default (DSCP = d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 01 01
1 : 01 01 01 01 01 01 01 02 02 02
2 : 02 02 02 02 03 03 03 03 03 03
3 : 03 03 04 04 04 04 04 04 04 04
4 : 05 05 05 05 05 05 05 05 06 06
5 : 06 06 06 06 06 06 07 07 07 07
6 : 07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)
TC: 0 1 2 3 4 5 6 7
-----
Threshold: 0 0 0 0 0 0 0 0

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues

```

Follow this example to view information about a specific port channel interface.

```

device# show qos interface port-channel 20
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 3/48
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
    In-CoS: 0 1 2 3 4 5 6 7
    -----
    Out-TC: 0 1 2 3 4 5 6 7
    Out-DP: 0 0 0 0 0 0 0 0

  TC-to-CoS Map: default
    In-TC: 0 1 2 3 4 5 6 7
    -----
    Out-CoS (DP=0): 0 1 2 3 4 5 6 7
    Out-CoS (DP=1): 0 1 2 3 4 5 6 7
    Out-CoS (DP=2): 0 1 2 3 4 5 6 7
    Out-CoS (DP=3): 0 1 2 3 4 5 6 7

  DSCP Mutation Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 01 02 03 04 05 06 07 08 09
    1 : 10 11 12 13 14 15 16 17 18 19
    2 : 20 21 22 23 24 25 26 27 28 29
    3 : 30 31 32 33 34 35 36 37 38 39
    4 : 40 41 42 43 44 45 46 47 48 49
    5 : 50 51 52 53 54 55 56 57 58 59
    6 : 60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
    1 : 1/0 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
    2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
    3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
    4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
    5 : 6/0 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
    6 : 7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    -----
    0 : 00 00 00 00 00 00 00 00 01 01
    1 : 01 01 01 01 01 01 02 02 02 02
    2 : 02 02 02 02 03 03 03 03 03 03
    3 : 03 03 04 04 04 04 04 04 04 04
    4 : 05 05 05 05 05 05 05 05 06 06
    5 : 06 06 06 06 06 06 07 07 07 07
    6 : 07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
    TC: 0 1 2 3 4 5 6 7
    -----
  Threshold: 0 0 0 0 0 0 0 0

  Flow control mode Off

  Per Traffic-Class Tail Drop Threshold (bytes)
    TC: 0 1 2 3 4 5 6 7
    -----
  Threshold: 0 0 0 0 0 0 0 0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues

```

[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

Interface Ethernet 3/2

Provisioning Mode: none

Default TC: 0

CoS-to-TC Map: default

In-CoS: 0 1 2 3 4 5 6 7

-----  
Out-TC: 0 1 2 3 4 5 6 7

Out-DP: 0 0 0 0 0 0 0 0

TC-to-CoS Map: default

In-TC: 0 1 2 3 4 5 6 7

-----  
Out-CoS (DP=0): 0 1 2 3 4 5 6 7

Out-CoS (DP=1): 0 1 2 3 4 5 6 7

Out-CoS (DP=2): 0 1 2 3 4 5 6 7

Out-CoS (DP=3): 0 1 2 3 4 5 6 7

DSCP Mutation Map: default (DSCP = d1d2)

d1 : d2 0 1 2 3 4 5 6 7 8 9

-----  
0 : 00 01 02 03 04 05 06 07 08 09

1 : 10 11 12 13 14 15 16 17 18 19

2 : 20 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

6 : 60 61 62 63

DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)

d1 : d2 0 1 2 3 4 5 6 7 8 9

-----  
0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0

1 : 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0 2/0

2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0

3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0

4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0 6/0

5 : 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0 7/0

6 : 7/0 7/0 7/0 7/0

DSCP-to-CoS Map: default (DSCP = d1d2)

d1 : d2 0 1 2 3 4 5 6 7 8 9

-----  
0 : 00 00 00 00 00 00 00 00 01 01

1 : 01 01 01 01 01 01 02 02 02 02

2 : 02 02 02 02 03 03 03 03 03 03

3 : 03 03 04 04 04 04 04 04 04 04

4 : 05 05 05 05 05 05 05 05 06 06

5 : 06 06 06 06 06 06 07 07 07 07

6 : 07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)

TC: 0 1 2 3 4 5 6 7

-----  
Threshold: 0 0 0 0 0 0 0 0

Flow control mode Off

...<output truncated>

Traffic Class Scheduler configured for 8 Strict Priority queues

[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

Interface Ethernet 1/41

Provisioning Mode: none

Default TC: 0

CoS-to-TC Map: default

In-CoS: 0 1 2 3 4 5 6 7

-----  
Out-TC: 0 1 2 3 4 5 6 7

Out-DP: 0 0 0 0 0 0 0 0

show qos interface port-channel

```
TC-to-CoS Map: default
      In-TC: 0  1  2  3  4  5  6  7
-----
Out-CoS (DP=0): 0  1  2  3  4  5  6  7
Out-CoS (DP=1): 0  1  2  3  4  5  6  7
Out-CoS (DP=2): 0  1  2  3  4  5  6  7
Out-CoS (DP=3): 0  1  2  3  4  5  6  7

DSCP Mutation Map: default (DSCP = d1d2)
d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   00 01 02 03 04 05 06 07 08 09
1 :   10 11 12 13 14 15 16 17 18 19
2 :   20 21 22 23 24 25 26 27 28 29
3 :   30 31 32 33 34 35 36 37 38 39
4 :   40 41 42 43 44 45 46 47 48 49
5 :   50 51 52 53 54 55 56 57 58 59
6 :   60 61 62 63

DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
1 :   1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
2 :   2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
3 :   3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 :   5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 :   6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
6 :   7/0 7/0 7/0 7/0

DSCP-to-CoS Map: default (DSCP = d1d2)
d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   00 00 00 00 00 00 00 00 01 01
1 :   01 01 01 01 01 01 02 02 02 02
2 :   02 02 02 02 03 03 03 03 03 03
3 :   03 03 04 04 04 04 04 04 04 04
4 :   05 05 05 05 05 05 05 05 06 06
5 :   06 06 06 06 06 06 07 07 07 07
6 :   07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)
      TC:      0      1      2      3      4      5      6      7
-----
Threshold:    0      0      0      0      0      0      0      0

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show qos interface ve

Displays QoS configuration information about a specific Virtual Ethernet interface.

## Syntax

```
show qos interface ve ve_number
```

## Parameters

*ve\_number*

A specific Virtual Ethernet number.

## Modes

Privileged EXEC mode.

## Examples

Follow this example to view information about a specific VE interface.

```

device# show qos interface ve 20
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ve 20
  Provisioning Mode: none

  DSCP Mutation Map: default (DSCP = d1d2)
    d1 : d2 0  1  2  3  4  5  6  7  8  9
    -----
    0 :   00 01 02 03 04 05 06 07 08 09
    1 :   10 11 12 13 14 15 16 17 18 19
    2 :   20 21 22 23 24 25 26 27 28 29
    3 :   30 31 32 33 34 35 36 37 38 39
    4 :   40 41 42 43 44 45 46 47 48 49
    5 :   50 51 52 53 54 55 56 57 58 59
    6 :   60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 : d2 0  1  2  3  4  5  6  7  8  9
    -----
    0 :   0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
    1 :   1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0 2/0
    2 :   2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0 3/0
    3 :   3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
    4 :   5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
    5 :   6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0 7/0
    6 :   7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 : d2 0  1  2  3  4  5  6  7  8  9
    -----
    0 :   00 00 00 00 00 00 00 00 00 01 01
    1 :   01 01 01 01 01 01 02 02 02 02 02
    2 :   02 02 02 02 03 03 03 03 03 03 03
    3 :   03 03 04 04 04 04 04 04 04 04 04
    4 :   05 05 05 05 05 05 05 05 05 06 06
    5 :   06 06 06 06 06 06 07 07 07 07 07
    6 :   07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
    TC:      0      1      2      3      4      5      6      7
    -----
  Threshold: 0      0      0      0      0      0      0      0

```

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos maps cos-traffic-class

Displays configured t CoS-to-traffic class mutation maps.

## Syntax

```
show qos maps cos-traffic-class
```

## Modes

Privileged EXEC mode.

## Examples

To display information on defined QoS CoS-to-traffic class mutation maps and where they are applied, use this command.

```
device# show qos maps cos-traffic-class

Cos-to-Traffic Class map 'cosTCMap'
In-Cos      : 0 1 2 3 4 5 6 7
-----
TrafficClass : 0 1 2 3 3 6 6 6
DropPrecedence: 0 0 0 0 0 1 0 1

Enabled on the following interfaces:
  Eth 1/4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos maps dscp-cos

Displays configured DSCP to CoS mutation maps.

## Syntax

`show qos maps dscp-cos`

## Modes

Privileged EXEC mode

## Examples

To display information on defined QoS DSCP to CoS mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-cos

Dscp-to-CoS map 'dscpCoS' (dscp= d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 01 01
1 : 01 01 01 01 01 01 02 02 02 02
2 : 02 02 02 04 03 03 03 03 03 03
3 : 03 03 04 04 04 04 04 04 04 04
4 : 05 05 05 05 05 05 05 05 06 06
5 : 06 06 06 06 06 06 07 07 07 07
6 : 07 07 07 07
```

Enabled on the following interfaces:  
Eth 1/3

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos maps dscp-mutation

Displays configured DSCP mutation maps.

## Syntax

```
show qos maps dscp-mutation
```

## Modes

Privileged EXEC mode

## Examples

To display information on defined QoS DSCP mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-mutation

Dscp-to-Dscp Mutation map 'dscpMut' (dscp= d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 :   00 01 02 03 04 05 06 07 08 09
1 :   10 11 12 13 14 15 16 17 18 19
2 :   20 21 22 23 24 25 26 27 28 29
3 :   30 31 32 33 34 35 36 37 38 39
4 :   40 41 42 43 44 45 46 47 48 49
5 :   50 51 52 53 54 55 56 57 58 59
6 :   40 61 62 63
```

```
Enabled on the following interfaces:
Eth 1/3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos maps dscp-traffic-class

Displays configured DSCP to traffic class mutation maps.

## Syntax

`show qos maps dscp-traffic-class`

## Modes

Privileged EXEC mode

## Examples

To display information on defined QoS DSCP to traffic class mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-traffic-class

Dscp-to-Traffic-Class map 'dscpTC'
{x/y: traffic-class = x, drop-precedence = y & dscp = d1d2}
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 4/2 1/0
1 : 1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
2 : 2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
3 : 3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 : 5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 : 6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
6 : 7/0 7/0 7/0 7/0
```

Enabled on the following interfaces:  
Eth 1/4

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos maps traffic-class-cos

Displays configured traffic class to CoS mutation maps.

## Syntax

```
show qos maps traffic-class-cos
```

## Modes

Privileged EXEC mode

## Examples

To display information on defined QoS DSCP to traffic class to CoS mutation maps and where they are applied, use this command.

```
device# show qos maps traffic-class-cos

Traffic Class-to-Cos map 'tcCoS' (drop-precedence = dp0 to dp3)
TrafficClass : 0 1 2 3 4 5 6 7
-----
Out-Cos (dp0) : 0 1 2 3 4 5 6 7
Out-Cos (dp1) : 0 1 2 3 4 5 6 7
Out-Cos (dp2) : 0 1 2 3 4 4 6 7
Out-Cos (dp3) : 0 1 2 3 4 5 6 7

Enabled on the following interfaces:
Eth 1/4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos-mpls maps dscp-exp

Displays configured QoS Multiprotocol Label Switching (MPLS) DSCP to EXP egress mutation maps.

## Syntax

`show qos-mpls maps dscp-exp`

## Modes

Privileged EXEC mode.

## Examples

To display information on defined QoS MPLS DSCP to EXP egress mutation maps and where they are applied, use this command.

```
device# show qos-mpls maps dscp-exp

dscp-exp map      'dscpExp' (dscp= d1d2)
d1      : d2 0  1  2  3  4  5  6  7  8  9
-----
0      :    0  0  2  0  0  0  0  0  0  1  1
1      :    1  1  1  1  1  1  2  2  2  2  2
2      :    2  2  2  2  3  3  3  3  3  3  3
3      :    3  3  4  4  4  4  4  4  4  4  4
4      :    5  5  5  5  5  5  5  5  6  6  6
5      :    6  6  6  6  6  6  7  7  7  7  7
6      :    7  7  7  0
```

Enabled on the following slots:  
Eth 1/4

## History

Release version	Command history
16r.1.00	This command was introduced.



# show qos-mpls maps exp-dscp

Displays configured QoS Multiprotocol Label Switching (MPLS) EXP to DSCP mutation maps.

## Syntax

```
show qos-mpls maps exp-dscp
```

## Modes

Privileged EXEC mode.

## Examples

To display information on defined QoS MPLS EXP to DSCP mutation maps and where they are applied, use this command.

```
device# show qos-mpls maps exp-dscp

exp-dscp map 'expDSCP'
  Exp   : 0 1 2 3 4 5 6 7
  -----
  DSCP  : 0 2 4 3 6 4 5 7
```

```
Enabled on the following slots:
  Eth 1/4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos-mpls maps exp-traffic-class

Displays configured QoS Multiprotocol Label Switching (MPLS) EXP to traffic class mutation maps.

## Syntax

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

## Modes

Privileged EXEC mode.

## Examples

To display information on defined QoS MPLS EXP to traffic class mutation maps and where they are applied, use this command.

```
device# show qos-mpls maps exp-traffic-class
```

```
exp-traffic-class map 'expTc'  
  Exp      :    0  1  2  3  4  5  6  7  
-----  
traffic-class : 5  5  4  6  5  5  5  5  
drop-precedence: 0  1  1  1  0  2  2  1
```

```
  Enabled on the following slots:  
    Eth 1/4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show qos-mpls maps traffic-class-exp

Displays configured QoS Multiprotocol Label Switching (MPLS) traffic class to EXP mutation maps.

## Syntax

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

## Modes

Privileged EXEC mode.

## Examples

To display information on defined QoS MPLS traffic class to EXP mutation maps and where they are applied, use this command.

```
device# show qos-mpls maps traffic-class-exp

traffic-class-exp map 'tcExp' (Drop-Precedence = dp)
dp: traffic-class : 0 1 2 3 4 5 6 7
-----
0: exp           : 0 1 2 3 4 0 6 7
1:               : 0 1 2 3 4 5 6 5
2:               : 0 1 2 3 4 5 6 7
3:               : 0 1 2 3 4 5 6 7
```

```
Enabled on the following slots:
  Eth 1/4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show route-map

Displays the PBR configuration details.

## Syntax

```
show route-map [ name | interface { ethernet slot/port | ve ve-number } ]
```

## Parameters

*name*

The name of the route-map.

interface { ethernet *slot/port*

Specifies the route-map configuration details on a specific interface.

ve *ve-number*

Specifies the route-map configuration details on a virtual Ethernet interface.

## Modes

Privileged EXEC mode

## Command Output

The **show port-security** command displays the following information:

Output field	Description
Active/Partial/Inactive	Indicates the instantiation of the route-map configuration into the underlying hardware. Possible meanings for inactive may be no room in the TCAM for programming the ACL, or the exhaustion of next-hop entries within the hardware next-hop table.
Selected	Indicates which of the configured next hops is currently being used by the policy. If the keyword selected is absent from the display, it indicates that none of the next hops in the list is being used and the packet is being routed by the standard routing mechanism.
Policy routing matches	Provides a summary of the number of times any of the match criteria within the specific ACL have been hit. If the ACL binding was unable to allocate a counter for the ACL (due to resource exhaustion) the count value will show "Counter not available" otherwise an actual counter value will be displayed.

## Examples

To display the route map information, enter the following command.

```
device# show route-map
Interface Ethernet 1/6
  ip policy route-map route1
```

To display the details of the configured routing attributes, enter the following command.

```
device# show route-map routel
Interface Ethernet 1/6
ip policy route-map routel permit 1 (Active)
  match ip address acl test1
  set ip next-hop 6.0.0.1 (selected)
Policy routing matches: 1443 packets
```

To display the route-map configuration details on a specific interface, enter the following command.

```
device# show route-map interface ethernet 1/6
Interface Ethernet 1/6
ip policy route-map routel permit 1 (Active)
  match ip address acl test1
  set ip next-hop 6.0.0.1 (selected)
Policy routing matches: 1543 packets
```

# show run router mpls cspf-group

Displays the CSPF fate-sharing group configuration for all groups configured on a device.

## Syntax

```
show run router mpls cspg-group group_name [ from | link | node [ ip_addr ] ] | subnet ip_addr/mask ]
```

## Parameters

**from** *ip\_addr*

Configures the CSPF group from the specified IP address.

**link** *ip\_addr*

Configures the CSPF group from and to the specified IP address.

**node** *ip\_addr*

Configures the CSPF group node IP address.

**subnet** *ip\_addr/mask*

Configures the CSPF group subnet address.

## Modes

EXEC mode.

## Examples

The following example displays the fate-sharing group configuration for all groups currently configured on the device.

```
device# show run router mpls cspf-group gold
cspf-group test8
penalty 65535
node 10.7.7.3
node 10.7.7.8
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config

Displays the contents of the running configuration.

## Syntax

```
show running-config
```

## Parameters

Refer to the Usage Guidelines.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display the running configuration. This is the configuration that is currently active on the local device but which is not saved persistently.

This command is supported only on the local device.

Enter **show running-config ?** to display the list of available configuration entries.

## Examples

The following command example displays the contents of the running configuration.

```
device# show running-config
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config aaa

Displays the configuration attributes for the authentication, authorization, and accounting (AAA) server from the configuration database.

## Syntax

```
show running-config aaa [ accounting [ commands | exec ] | authentication [ login ] ]
```

## Parameters

### accounting

Configures Login or Command accounting

### commands

Enable/Disable Command accounting

### exec

Enable/Disable Login accounting

### authentication

Configures preferred order of Authentication output modifiers

### login

Configures the order of sources for login (default = 'local')

## Modes

Privileged EXEC mode

## Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

## Examples

To display the authentication mode:

```
device# show running-config aaa
aaa authentication radius local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none

device# show running-config aaa authentication
aaa authentication login radius local

device# show running-config aaa authentication
aaa authentication login ldap local-auth-fallback
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config aaa accounting

Displays the AAA server accounting configuration.

## Syntax

`show running-config aaa accounting`

## Modes

Privileged EXEC mode

## Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

## Examples

To displaying the authentication mode:

```
device# show running-config aaa accounting
aaa accounting exec default start-stop tacacs+
aaa accounting commands default start-stop tacacs+
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config access-list overlay type vxlan

Displays the ACL configuration.

## Syntax

```
show running-config access-list overlay type vxlan { standard | extended } [ overlay_vxlan_acl_name ]
```

## Parameters

### standard

Specifies standard..

### extended

Specifies extended..

### overlay\_vxlan\_acl\_name

Specifies the overlay VXLAN ACL name.

## Modes

EXEC mode

## Usage Guidelines

## Command Output

The **show running-configuration access-list overlay type** command displays the following information:

## Examples

```
device# show running-config access-list overlay type vxlan extended overlay_vxlan_ext
overlay access-list type vxlan extended overlay_vxlan_ext
seq 10 permit dst-vtep-ip 10.1.1.1 src-vtep-ip any vni 5 native dst-ip any src-ip 100.1.1.1 dst-port
any src-port 5555 count sflow (Active)
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config event-handler

Displays details of all event-handler profiles defined on the device. You can filter the results by trigger ID or details. You can also filter the results by Python-script actions.

## Syntax

```
show running-config event-handler [ event-handler-name ]
show running-config event-handler action [ event-handler-name ] [ python-script [ file-name ] ]
show running-config event-handler trigger [ event-handler-name ] [ trigger-id [ raslog raslog-id ] ]
```

## Parameters

*event-handler-name*

Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

**action** *python-script* *file-name*

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

**trigger** *trigger-id*

Specifies an event-handler trigger. When the trigger-condition occurs, a Python script is run.

**raslog** *raslog-id*

Specifies a RASlog message ID as the trigger.

## Modes

Privileged EXEC mode

## Command Output

The **show running-config event-handler** command displays the following information:

Output field	Description
event-handler	Displays the event-handler name.
action python-script	Displays the name of the Python script called if the event handler is triggered.

## Examples

The following example displays the actions assigned to all event handlers.

```
device# show running-config event-handler action
event-handler evh1
action python-script pyth1.py
!
event-handler evh2
action python-script pyth.py
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config ip access-list

Displays a list of IPv4 ACLs defined on the switch, including the rules they contain.

## Syntax

```
show running-config ip access-list [ { standard | extended } [ ACL_name ] ]
```

## Parameters

### standard

Specifies the standard ACL type.

### extended

Specifies the extended ACL type.

### ACL\_name

Specifies the ACL name.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all IPv4 ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of IPv4 ACLs bound to interfaces, use the **show access-list ip** command.

## Examples

The following example displays the IPv4 ACLs defined on the switch.

```
device# show running-config ip access-list

ip access-list standard stdACL3
  seq 5 permit host 10.20.33.4
  seq 7 permit any
ip access-list extended extdACL5
  seq 5 deny tcp host 10.24.26.145 any eq 23
  seq 7 deny tcp any any eq 80
  seq 10 deny udp any any range 10 25
  seq 15 permit tcp any
ip access-list extended extdACLwithNoRules
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config ipv6

Displays global ipv6 configurations.

## Syntax

```
show running-config ipv6 [ access-list [ extended | standard ] ipv6-acl-name seq sequence-number ]
```

```
show running-config ipv6 [ import routes ]
```

```
show running-config ipv6 [ nd [ global-suppress-ra | ra-dns-server | ra-domain-name ]]
```

```
show running-config ipv6 [ prefix-list [ ge | le ] prefix-length ]
```

```
show running-config ipv6 [ protocol [ vrrp | vrrp-extended ]]
```

```
show running-config ipv6 [ receive access-group ]
```

```
show running-config ipv6 [ route ]
```

```
show running-config ipv6 [ router ospf [ vrf ]]
```

## Parameters

### access-list

Specifies the access-control list (ACL).

### extended

Specifies the extended IP ACL.

### standard

Specifies the standard IP ACL.

### *ipv6-acl-name*

The IPv6 ACL name.

### seq *sequence-number*

Specifies the sequence number.

### import routes

Specifies import IPv6 routes.

### nd

Displays neighbor discovery commands.

### global-suppress-ra

Sets the suppress-ra option globally .

### ra-dns-server

Sets the global DNS server option applied on all ND6.

### ra-domain-name

Set the global domain name option that applied on all ND6 interfaces.

### prefix-list

Specifies the prefix-list.

### ge

Specifies the minimum IPv6 prefix length.

**prefix-length**

The IPv6 prefix length. The range is from 1 through 128.

**le**

Specifies the maximum IPv6 prefix length.

**protocol**

Set the global domain name option that applied on all ND6 interfaces.

**vrrp**

Specifies the Virtual Router Redundancy Protocol IPv6 (VRRPv3).

**vrrp-extended**

Specifies the Virtual Router Redundancy Protocol IPv6 Extended (VRRPv3-E).

**receive**

Specifies the receive ACL.

**access-group**

Specifies to bind or unbind the existing ACL.

**route**

Specifies the IPv6 unicast static route.

**router**

Specifies the IPv6 router.

**ospf**

Specifies the Open Shortest Path First (OSPF) version 3.

**vrf**

Specifies the VRF instance.

## Modes

Privileged EXEC mode

## Examples

The following is an example of the **show running-config ipv6** command output.

```
device# show running-config ipv6
ipv6 route 3063:6363::/64 fe80::52eb:1aff:fe97:cf51 ve 4050
ipv6 nd ra-dns-server 2000:1234:122:ffff::ffee
ipv6 nd ra-dns-server 3500:35:0:35::1
ipv6 nd ra-domain-name extreme.com
ipv6 nd ra-domain-name user.co.in
ipv6 nd ra-domain-name netiron.com
```

## History

Release version	Command history
16.1.00	This command was introduced.



# show running-config ipv6 access-list

Displays a list of IPv6 ACLs defined on the switch, including the rules they contain.

## Syntax

```
show running-config ipv6 access-list [ { standard | extended } [ ACL_name ] ]
```

## Parameters

### standard

Specifies the standard ACL type.

### extended

Specifies the extended ACL type.

### ACL\_name

Specifies the ACL name.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all IPv6 ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of all IPv6 ACLs bound to interfaces, use the **show access-list ipv6** command.

## Examples

The following example displays all standard IPv6 ACLs defined on the switch:

```
device# show running-config ipv6 access-list standard
ipv6 access-list standard distList
  seq 10 deny 2001:125:132:35::/64
  seq 20 deny 2001:54:131::/64
  seq 30 deny 2001:5409:2004::/64
  seq 40 permit any
!
ipv6 access-list standard ipv6_acl_std_1
  seq 10 deny 2001:2001::/64 count log
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config mac access-list

Displays a list of MAC ACLs defined on the switch, including the rules they contain.

## Syntax

```
show running-config mac access-list [ { standard | extended } [ ACL_name ] ]
```

## Parameters

### standard

Specifies the standard ACL type.

### extended

Specifies the extended ACL type.

### ACL\_name

Specifies the ACL name.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all MAC ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of all MAC ACLs bound to interfaces, use the **show access-list mac** command.

## Examples

The following example displays all MAC ACLs defined on the switch.

```
device# show running-config mac access-list
mac access-list standard stdmacaclin
seq 11 permit 1111.1112.1113 7777.7777.7777 count log
seq 12 permit 1111.1112.1114 7777.7777.7777 count log
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config password-attributes

Displays global password attributes.

## Syntax

```
show running-config password-attributes [ admin-lockout ] [ max-lockout-duration ] [ max-retry ] [ min-length ]
```

```
show running-config password-attributes character-restriction [ lower | numeric | special-char | upper ]
```

## Parameters

### admin-lockout

Displays lockout for admin role accounts.

### max-retry

Displays the number of failed password logins permitted before a user is locked out. Values range from 0 through 16 attempted logins. The default value is 0.

### min-length

Displays the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

### max-lockout-duration

Displays the maximum number of minutes after which the user account is unlocked. Range is from 0 through 99999. The default is 0, representing an infinite duration.

### character-restriction

Displays the restriction on various types of characters.

#### lower

Displays the minimum number of lowercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

#### numeric

Displays the minimum number of numeric characters that must occur in the password. Values range from 0 through 32 characters. The default is 0.

#### special-char

Displays the number of punctuation characters that must occur in the password. All printable, nonalphanumeric punctuation characters, except colon (:) are allowed. Values range from 0 through 32 characters. The default value is 0.

#### upper

Displays the minimum number of uppercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

## Modes

Privileged EXEC mode

## Usage Guidelines

The attributes are not displayed when they hold default values.

## Examples

The following example displays all global password attributes.

```
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
password-attributes max-lockout-duration 5000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config radius-server

Displays the local device configuration for the RADIUS server from the configuration database.

## Syntax

```
show running-config radius-server host { ip-address | hostname }
```

## Parameters

### host

Identifies the RADIUS server by host name or IP address.

#### *hostname*

Specifies the host name of the RADIUS server.

#### *ip-address*

Specifies the IP address of the RADIUS server. IPv4 and IPv6 are supported.

## Modes

Privileged EXEC mode

## Examples

```
device# show running-config radius-server host 10.38.37.180
```

```
radius-server host 10.38.37.180
```

```
protocol pap
```

```
key changedsec
```

```
timeout 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config rmon

Displays Remote Monitor configuration information.

## Syntax

```
show running-config rmon [ alarm | event ]
```

## Parameters

### alarm

Displays the Remote Monitor alarm configuration.

### event

Displays the Remote Monitor event configuration

## Modes

Privileged EXEC mode

# show running-config role

Displays name and description of the configured roles.

## Syntax

```
show running-config role [ name role_name [ desc ] ]
```

## Parameters

**name** *role\_name*

Displays roles defined for users.

**desc**

Displays role descriptions.

## Modes

Privileged EXEC mode

## Examples

The following example displays all roles configured on the device.

```
device# show running-config role

role name VLANAdmin desc "Manages security CLIs"
role name NetworkAdmin desc "Manages Network CLIs"
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config rule

Displays configured access rules.

## Syntax

```
show running-config rule [ index ]
```

```
show running-config rule index { action | command command_name | operation | role }
```

```
show running-config rule { action { reject | accept } | command command_name | operation { read-only | read-write } | role role-name }
```

## Parameters

*index*

Displays the rule with the specified index number. Values range from 1 through 512.

**action reject | accept**

Following the *index* parameter, indicates whether **reject** or **accept** is specified for that rule. If the *index* parameter is not specified, displays all rules with the specified action.

**command** *command\_name*

Displays rule configuration for the specified command. To display a list of supported commands, type a question mark (?). This list varies according to whether or not you specify a rule index.

**operation read-only | read-write**

Following the *index* parameter, indicates whether **read-only** or **read-write** is specified for that rule. If the *index* parameter is not specified, displays all rules with the specified operation.

**role** *role-name*

Displays rule configuration for the specified role.

## Modes

Privileged EXEC mode



## Examples

The following example displays the configured roles and their rules.

```
device# show running-config rule

rule 30 action accept operation read-write role NetworkSecurityAdmin
rule 30 command role
!
rule 31 action accept operation read-write role NetworkSecurityAdmin
rule 31 command rule
!
rule 32 action accept operation read-write role NetworkSecurityAdmin
rule 32 command username
!
rule 33 action accept operation read-write role NetworkSecurityAdmin
rule 33 command aaa
!
rule 34 action accept operation read-write role NetworkSecurityAdmin
rule 34 command radius-server
!
rule 35 action accept operation read-write role NetworkSecurityAdmin
rule 35 command configure
```

The following example displays a single rule.

```
device# show running-config rule 30

rule 30
  action accept operation read-write role NetworkSecurityAdmin command role
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config ssh

Displays the Secure Shell (SSH) status in the running-config.

## Syntax

`show running-config ssh`

## Modes

Privileged EXEC mode

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config ssh server

Displays the SSH server status in the running-config.

## Syntax

```
show running-config ssh server
```

## Modes

Privileged EXEC mode

## Usage Guidelines

SSH server configuration is placed at the beginning of the running-config and is part of the global configuration of the device. SSH is enabled by default and no entry is shown in the running-config when set to default.

## Examples

When SSH service is shut down:

```
device# show running-config ssh server
ssh server shutdown
device# show running-config ssh server
ssh server shutdown
ssh server key-exchange dh-group-14
```

When SSH service is enabled:

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config ssh server key-exchange

Displays the SSH server key-exchange status in the running-config.

## Syntax

`show running-config ssh server key-exchange`

## Modes

Privileged EXEC mode

## Examples

Typical command output:

```
device# show running-config ssh server key-exchange
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange is configured to DH Group 14:

```
device# show running-config ssh server key-exchange
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange method has the default value:

```
device# show running-config ssh server key-exchange
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show running-config username

Displays the user accounts on the device.

## Syntax

```
show running-config username [ username ] [ access-time ] [ desc ] [ enable ] [ encryption-level ] [ expire ] [ password ] [ role ]
```

## Parameters

### *username*

Displays the configuration of a specified username. The maximum number of characters is 40.

### **access-time**

Displays access-time configuration.

### **desc**

Displays the description of the user configuration.

### **enable**

Displays the account enablement status.

### **encryption-level**

Password encryption level. Values are 0 through 7. The default is 0.

### **expire**

Date until the password remains valid in YYYY-MM-DD format. Valid year values range from 1902 through 2037. By default, passwords do not expire.

### **password**

Account password.

### **role**

The role associated with the account.

## Modes

Privileged EXEC mode

## Usage Guidelines

To display details for one user only, specify *username* . Otherwise, this command displays all user accounts on the device.

Use the various parameters to query the specified account details.

This command does not display the root account.

Defaults are not displayed.

## Examples

The following example displays the user accounts on the device.

```
device# show running-config username  
  
username admin password "BwrsDbB+tABWGwPINOVKoQ==\n" encryption-level 7 role admin desc Administrator  
username user password "BwrsDbB+tABWGwPINOVKoQ==\n" encryption-level 7 role user desc User
```

The following example displays a specific user account.

```
device# show running-config username admin  
  
username admin password "BwrsDbB+tABWGwPINOVKoQ==\n" encryption-level 7 role admin desc Administrator
```

The following example displays the enabled status for a specific user account.

```
device# show running-config username admin enable  
  
username admin enable true
```

The following example displays user access on the device.

```
device# show running-config username access-time  
username admin access-time ""  
username extremel access-time 0000  
username user access-time ""  
username user1 access-time 1700
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show sflow

Displays sFlow configuration information and statistics.

## Syntax

```
show sflow interface | all
```

## Command Default

sFlow is disabled on all interfaces.

## Parameters

**all**

Displays all sFlow information and statistics.

**interface**

Displays sFlow information for an Ethernet interface.

## Modes

Privileged EXEC mode

## Examples

The following example displays all sFlow statistics.

```
device# show sflow all

sFlow services are:                               enabled
Global default sampling rate:                     32768 pkts
Global default counter polling interval:          20 secs
Collector server address
-----
3ffe:1900:4545:3:200:f8ff:fe21:67cf : 6343      0
fe80::200:f8ff:fe21:67cf      : 6343      0
192.35.41.32      : 6343      0
fe80::201:fdff:fe21:43cd      : 6343      0
192.44.23.45      : 6343      0

Number of samples sent
-----
```

# show slots

Displays the slot information for the SLX-OS device.

## Syntax

**show slots**

## Modes

Privileged EXEC mode

## Command Output

The **show slots** command displays the following information:

Output field	Description
Slot	Slot numbers of the device. <ul style="list-style-type: none"> <li>• M1 and M2—Slots for Management Module (MM)</li> <li>• S1 through S6—Slots for the Switch Fabric Module (SFM)</li> <li>• L1 through L4—Interface module slots for an SLX 9850-4 chassis</li> <li>• L1 through L8—Interface module slots for an SLX 9850-8 chassis</li> </ul>
Type	Module type and version as described in the Description field: <ul style="list-style-type: none"> <li>• MM</li> <li>• SFM</li> <li>• LC36X100G—36-port 100GbE interface module (line card)</li> <li>• LC72X10G—72-port 10GbE interface module (line card)</li> </ul>
Description	Module description.
ID	Module ID: <ul style="list-style-type: none"> <li>• 179—MM</li> <li>• 183—SFM for an SLX 9850-4 router.</li> <li>• 187—SFM for an SLX 9850-8 router.</li> <li>• 180—72-port 10GbE interface module</li> <li>• 181—36-port 100GbE interface module</li> </ul>
Status	Status of the module as one of the following: <ul style="list-style-type: none"> <li>• DIAG RUNNING POST1—The module is present, powered on, and running the POST (power-on self-test). This status is not valid for the management modules.</li> <li>• DIAG RUNNING POST2—The module is present, powered on, and running the reboot power on self tests. This status is not valid for the management modules.</li> <li>• DISABLED—The module is powered on but disabled.</li> <li>• ENABLED—The module is on and fully enabled.</li> <li>• FAULTY—The module is faulty because an error is detected.</li> <li>• INITIALIZING—The module is present, powered on, and initializing hardware components.</li> <li>• LOADING—The module is present, powered on, and loading the initial configuration.</li> <li>• POWERED-OFF—The module is present in the slot but is powered off.</li> <li>• POWERING UP—The module is present and powering on.</li> </ul>



Output field	Description
	<ul style="list-style-type: none"> <li>UNKNOWN—The module is inserted but its state cannot be determined.</li> <li>UNLATCHED—The module is inserted but it is not secured to the chassis with its captive screws. This status is supported for SFMs, 72-port 10GbE module, and the 36-port 100GbE module.</li> <li>VACANT—The slot is empty.</li> </ul>

## Examples

The following example shows the slot information for an SLX 9850-4 router.

```

device# show slots
Slot  Type           Description                ID      Status
-----
M1    MM v5              Management Module          179     ENABLED
M2                                 VACANT
S1                                 VACANT
S2    SFM4 v4            Switch Fabric Module       183     ENABLED
S3                                 VACANT
S4    SFM4 v4            Switch Fabric Module       183     ENABLED
S5    SFM4 v4            Switch Fabric Module       183     ENABLED
S6                                 VACANT
L1    LC36x100G v3      36-port 100GE card        181     ENABLED
L2    LC72X10G v5       72-port 10GE card         180     ENABLED
L3    LC36x100G v3      36-port 100GE card        181     ENABLED
L4                                 UNLATCHED

```

## History

Release version	Command history
16r.1.00	This command was introduced for SFMs.
16r.1.01	This command was modified to add line cards and add the UNLATCHED status for SFMs.

# show spanning-tree

Displays Spanning Tree Protocol (STP) information.

## Syntax

```
show spanning-tree [ brief | interface { ethernet slot/port | port-channel port_channel_number } | pvst | mst [ brief | detail |  
instance instance_id | interface ] mst-config | vlan vlan_id ]
```

## Parameters

### brief

Display brief spanning tree information.

### interface

Display information about the spanning tree configuration on an interface.

### ethernet *slot/port*

Display spanning tree information about a specific Ethernet interface.

### port-channel *port\_channel\_number*

Display spanning tree information about a port channel interface.

### pvst

Display PVST+ information.

### mst

Display MSTP information.

### detail

Display detailed MSTP tree information.

### instance *instance\_id*

Display MSTP information about a specific instance.

### mst-config

Display MSTP region configuration information.

### vlan *vlan\_id*

Display spanning tree information about a specific VLAN.

## Modes

Privileged EXEC mode.

## Usage Guidelines

### NOTE

Extreme Networks supports the PVST+ and R-PVST+ protocols. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

## Examples

To display spanning tree information:

```
device# show spanning-tree brief
```

```
Spanning-tree Mode: Spanning Tree Protocol
```

```
Root ID      Priority 4096
             Address 768e.f805.5800
             Hello Time 8, Max Age 25, Forward Delay 20
```

```
Bridge ID    Priority 4096
             Address 768e.f805.5800
             Hello Time 8, Max Age 25, Forward Delay 20
```

Interface	Role	Sts	Cost	Prio	Link-type	Edge
Eth 2/32	DES	FWD	2000	128	P2P	No
Eth 2/66	DES	FWD	2000	128	P2P	No
Po 7	DES	FWD	2000	128	P2P	No
Po 8	DES	FWD	2000	128	P2P	No
Po 21	DES	LIS	500	128	P2P	No
Po 141	BKUP	BLK	1000	128	P2P	No
Po 151	DES	FWD	10000	128	P2P	No
Po 154	DES	FWD	285	128	P2P	No
Po 172	BKUP	BLK	1000	128	P2P	No
Po 173	BKUP	BLK	500	128	P2P	No

## History

Release version	Command history
16r.1.00	This command was introduced.

# show startup-config

Displays the contents of the startup configuration.

## Syntax

`show startup-config`

## Modes

Privileged EXEC mode

## Usage Guidelines

This command is supported only on the local device.

## Examples

The following example displays the contents of the startup configuration file.

```
device# show startup-config
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show statistics access-list

For a given network protocol and inbound/outbound direction, displays ACL statistical information. You can show statistics for a specified ACL or only for that ACL on a specified interface. You can also display statistical information for all ACLs bound to a specified device interface, VLAN or VE. You can also display statistical information for IPv4 or IPv6 receive-path ACLs.

## Syntax

```
show statistics access-list interface { ethernet slot / port | port-channel index | ve vlan_id | vlan vlan_id } { in | out }
show statistics access-list { ip | ipv6 } name interface [ ethernet slot / port | port-channel index | ve vlan_id ] { in | out }
show statistics access-list mac name interface [ ethernet slot / port | port-channel index | vlan vlan_id ] { in | out }
show statistics access-list receive { ip | ipv6 }
```

## Parameters

### interface

Filter by interface.

### ethernet

Specifies a physical Ethernet interface.

*slot*

Specifies a valid slot number.

*port*

Specifies a valid port number.

### port-channel *index*

Specifies a port-channel interface.

### ve *vlan\_id*

Specifies a virtual Ethernet (VE) interface.

### vlan *vlan\_id*

Specifies a VLAN interface.

### in | out

Specifies the ACL binding direction (incoming or outgoing).

### ip | ipv6 | mac

Specifies the network protocol.

*name*

Specifies the ACL name.

### receive

Specifies IPv4 or IPv6 receive-path traffic.

## Modes

Privileged EXEC mode

## Usage Guidelines

Statistics are displayed only for rules that contain the **count** keyword.

## Command Output

The **show statistics access-list** command displays the following information:

Output field	Description
Uncount	The counter resource is not allocated. This is typically seen if counting is not supported or if the hardware resources limit is reached.
Unwritten	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

## Examples

The following example displays inbound ACL statistics for a named IPv4 ACL.

```
device# show statistics access-list ip l3ext in
ip access-list l3ext Ethernet 1/8 in
seq 76 deny ip 10.10.75.10 0.0.0.0 any count log (795239 frames)
seq 77 hard-drop ip 10.10.75.10 0.0.0.0 10.10.11.0 0.0.0.255 count log (0 frames)
seq 78 hard-drop ip any 10.10.11.0 0.0.0.255 count log (0 frames)
seq 79 hard-drop ip any 10.10.0.0 0.0.255.255 count log (0 frames)
seq 80 hard-drop ip 10.10.75.10 0.0.0.0 any count log (0 frames)
seq 81 hard-drop ip 10.10.75.0 0.0.0.0 10.10.0.0 0.0.255.255 count log (0 frames)
seq 91 hard-drop ip any any count (0 frames)
seq 100 deny udp 10.10.75.0 0.0.0.255 10.10.76.0 0.0.0.255 count log (0 frames)
seq 1000 permit ip any any count log (0 frames)
```

The following example displays inbound ACL statistics for a specified interface. The ACL named `ipv6-std-acl` is applied on interface `4/1` to filter incoming routed traffic only.

```
device# show statistics access-list interface ethernet 4/1 in
ipv6 routed access-list ipv6-std-acl on Ethernet 4/1 at Ingress (From User)
  seq 10 permit host 0:1::1
  seq 20 deny 0:2::/64
  seq 30 deny any count (100 frames)
```

The following example displays inbound statistics for all ACLs bound to a specified VE interface.

```
device# show statistics access-list interface ve 3010 in
ipv6 access-list ip_acl_3 on Ve 3010 at Ingress (From User)
  seq 10 deny ipv6 2001:3010:131:35::/64 2001:1001:1234:1::/64 count (0 frames)
  seq 20 permit ipv6 2001:3010:131:35::/64 2001:3001:1234:1::/64
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show statistics access-list overlay type vxlan

Displays the statistics for each of the filter if filter has statistics enabled.

## Syntax

```
show statistics access-list overlay type vxlan user-acl-name
```

## Parameters

*user-acl-name*

The access list name.

## Modes

Privileged EXEC mode

## Examples

```
device# show statistics access-list overlay type vxlan abc_ext
Number of Rules: 2
seq 1000 permit dst-vtep-ip-host 200.1.1.1 src-vtep-ip-host 150.1.1.1 vni 1 vni-mask 0 redirect
Ethernet 2/65 sflow count 0(pkts)/0(bytes)
seq 1010 permit dst-vtep-ip-host 200.1.1.2 src-vtep-ip-host 150.1.1.2 vni 2 vni-mask 0 redirect
Ethernet 2/19 sflow count 44024773(pkts)/52829727600(bytes)
```

```
device# show access-list overlay transit tr_name
Overlay Transit Global Binding
  Inbound access-list is abc_ext (From User)
  Outbound access-list is not set
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show statistics bridge-domain

Displays statistics for logical interfaces in bridge domains.

## Syntax

```
show statistics bridge-domain bd-id
```

## Parameters

*bd-id*

The bridge domain ID.

## Modes

Privileged EXEC mode

## Usage Guidelines

```
show statistics bridge-domain bd- id
```

## Command Output

The **show statistics bridge-domain** command displays the following information:

Field	Description
Interface	The interface whose counter statistics are displayed.
RxPkts	The number of packets received at the specified interface.
RxBytes	The number of bytes received at the specified interface.
TxPkts	The number of packets transmitted from the specified interface.
TxBytes	The number of bytes transmitted from the specified interface.

## Examples

The following example displays statistics for all logical interfaces in all bridge domains.

```
device# show statistics bridge-domain
```

```
Bridge Domain 1 Statistics
```

Interface	RxPkts	RxBytes	TxPkts	TxBytes
eth 1/1.100	821729	821729	95940360	95940360
eth 1/21.200	884484	885855	95969584	95484555
po 1.300	8884	8855	9684	9955

```
Bridge Domain 20 Statistics
```

Interface	RxPkts	RxBytes	TxPkts	TxBytes
eth 1/6.400	821729	821729	95940360	95940360
eth 1/21.100	8884	8855	9684	9955
po 2.40	884484	885855	95969584	95484555



The following example displays statistics for all logical interfaces in the bridge domain 1.

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

```
Bridge Domain 1 Statistics
Interface          RxPkts      RxBytes      TxPkts      TxBytes
eth 1/1.100        821729      821729       95940360    95940360
eth 1/21.200       884484      885855       95969584    95484555
po 1.300           8884        8855         9684        9955
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# show statistics vlan

Displays the statistics for all ports and port channels on configured VLANs.

## Syntax

```
show statistics vlan vlan id
```

## Parameters

*vlan ID*

The specific VLAN ID.

## Modes

Privileged EXEC mode

## Usage Guidelines

```
show statistics vlan vlan- id
```

## Command Output

The **show statistics vlan** command displays the following information:

Field	Description
Interface	The interface whose counter statistics are displayed.
RxPkts	The number of packets received at the specified port.
RxBytes	The number of bytes received at the specified port.
TxPkts	The number of packets transmitted from the specified port.
TxBytes	The number of bytes transmitted from the specified port.

## Examples

The following example displays statistics for all ports and port channels on configured VLANs.

```
device# show statistics vlan
```

```
Vlan 10 Statistics
Interface      RxPkts          RxBytes          TxPkts          TxBytes
eth 1/1        821729          821729          95940360        95940360
eth 1/2        884484          885855          95969584        95484555
po 1           8884            8855            9684            9955

Vlan 20 Statistics
Interface      RxPkts          RxBytes          TxPkts          TxBytes
eth 1/6        821729          821729          95940360        95940360
eth 1/21       8884            8855            9684            9955
po 2           884484          885855          95969584        95484555
```

The following example displays statistics for all ports and port channels in the VLAN 10.

```
device# show statistics vlan 10
```

```
Vlan 10 Statistics
Interface      RxPkts      RxBytes      TxPkts      TxBytes
eth 1/1        821729      821729      95940360    95940360
eth 1/2        884484      885855      95969584    95484555
po 1           8884        8855        9684        9955
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# show storm-control

Displays all BUM (broadcast, unknown unicast and multicast)-related configurations in the system.

## Syntax

**show storm-control**

**show storm-control** [ **broadcast** | **multicast** | **unknown-unicast** ] [ **interface** { **ethernet** } *slot/port* ]

## Parameters

**storm-control**

Displays all BUM-related configurations in the system.

**broadcast**

Displays all BUM-related configurations in the system for the broadcast traffic type.

**interface**

Displays all BUM-related configurations in the system for the specified interface.

**ethernet**

Represents a valid, physical Ethernet port.

*slot/port*

Specifies a valid slot and port number.

**multicast**

Displays all BUM-related configurations in the system for the multicast traffic type.

**unknown-unicast**

Displays all BUM-related configurations in the system for the unknown-unicast traffic type.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display BUM storm-control-related configuration for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interface.

## Examples

To display storm control information for broadcast traffic on an Ethernet interface:

```
device# show storm-control broadcast interface ethernet 2/1

Interface  Type          rate (Mbps)  conformed   violated    total
Et 2/1    broadcast     100,000     12500000000 12500000000 25000000000
```

To display storm control information for all traffic on an Ethernet interface.

```
device# show storm-control interface ethernet 2/1

Interface  Type          rate (Mbps)  conformed   violated    total
Et 2/1    broadcast     100,000     12500000000 12500000000 25000000000
Et 2/1    unknown-unicast 100,000     12500000000 12500000000 25000000000
Et 2/1    multicast     100,000     12500000000 12500000000 25000000000
```

To display storm control information for all traffic in the system:

```
device# show storm-control

Interface  Type          rate (Mbps)  conformed   violated    total
Et 2/1    broadcast     100,000     12500000000 12500000000 25000000000
Et 2/1    unknown-unicast 100,000     12500000000 12500000000 25000000000
Et 2/1    multicast     100,000     12500000000 12500000000 25000000000
Et 2/2    broadcast     100,000     12500000000 12500000000 25000000000
Et 2/3    broadcast     100,000     12500000000 12500000000 25000000000
Et 2/4    unknown-unicast 100,000     12500000000 12500000000 25000000000
```

To display storm control information for all broadcast traffic the system:

```
device# show storm-control broadcast

Interface  Type          rate (Mbps)  conformed   violated    total
Et 2/1    broadcast     100,000     12500000000 12500000000 25000000000
Et 2/2    broadcast     100,000     12500000000 12500000000 25000000000
Et 2/3    broadcast     100,000     12500000000 12500000000 25000000000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show tm voq-stat ingress-device all discards

Displays ingress QoS queue discard statistics.

## Syntax

```
show tm voq-stat ingress-device all discards [ max-display max_display_number | priority traffic_class [ max-display max_display_number ] ]
```

## Parameters

### max-display

Limits the display of discards.

*max\_display\_number*

The discard display limit. The values range from one to a maximum of 32.

### priority

Displays discards by their traffic class priority.

*traffic\_class*

Traffic class priorities range from 0 through 7.

## Modes

Privileged EXEC mode.

## Usage Guidelines

The entries are sorted by the highest number of discards with eight entries displayed by default.

## Examples

Follow this example to show traffic management VOQ ingress discard statistics.

```
device# show tm voq-stat ingress-device all discards
```

```
-----SLOT 3 TOWER 2-----
Dest Port | Prio | Queue | Discards
-----
```

Dest Port	Prio	Queue	Discards
3/1	0	320	2473804
2/4	0	224	1867789
4/2	2	434	1023452
4/8	4	487	920349
1/2	1	120	858723
1/3	1	128	75328
2/5	0	260	22234
2/6	0	268	5248

Follow this example to show traffic management VOQ ingress discard statistics for a specific traffic class priority.

```
device# show tm voq-stat ingress-device all discards priority 0
```

```
-----SLOT 3 TOWER 2-----
Dest Port | Prio | Queue | Discards
-----
3/1       | 0    | 320   | 2473804
2/4       | 0    | 224   | 1867789
2/5       | 0    | 260   | 22234
2/6       | 0    | 268   | 5248
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show tm voq-stat ingress-device ethernet

Displays traffic management VOQ statistics for a specific ingress Ethernet interface.

## Syntax

```
show tm voq-stat ingress-device ethernet slot/port { discards [ max-display max_display_number | priority traffic_class ] |  
egress-port ethernet slot/port [ priority traffic_class ] | max-buffer-util | max-queue-depth [ max-display  
max_display_number | min-threshold minimum_threshold [ max-display max_display_number | priority traffic_class ] |  
priority traffic_class ] }
```

## Parameters

*slot/port*

The Ethernet slot and port

**discards**

Specifies discarded

**max-display**

Limits the display of discards.

*max\_display\_number*

The discard display limit. The values range from one to a maximum of 32.

**priority**

Displays discards by their traffic class priority.

*traffic\_class*

Traffic class priorities range from 0 through 7.

**egress-port** *slot/port*

The outbound port.

**max-buffer-util**

Displays a summary of traffic management VOQ maximum buffer utilization.

**max-queue-depth**

Displays a summary of traffic management VOQ maximum queue depth statistics.

**max-display**

Limit the output to a maximum number of display entries

*max\_display\_number*

The output that the display is limited to. The range is from 1 to 64 entries.

**min-threshold**

Specifies that the results leave out **max-queue-depths** below the minimum Byte threshold.

*minimum\_threshold*

The minimum threshold filter value in bytes. The range is from 1 to 1048640.

## Modes

Privileged EXEC mode.



## Examples

Follow this example to display traffic management VOQ statistics for an egress interface.

```
device# show tm voq-stat ingress-device ethernet 2/1 egress-port ethernet 2/7 priority 2
```

```
VOQ-Counters:
```

```
=====
```

```
Priority 2
```

```
-----
EnQue Pkt Count          67404602
EnQue Bytes Count       1768413221
Total Discard Pkt Count      0
Total Discard Bytes Count    0
Current Queue Depth        0
Maximum Queue Depth since Last read 160
```

Follow this example to display a summary of traffic management VOQ maximum queue depth statistics for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 max-queue-depth
```

```
----- Ports 1/1 - 1/36 -----
Dest Port | Prio | Queue | Max Depth | Max Util
-----|-----|-----|-----|-----
3/1       | 0    | 320   | 1013804  | 96%
2/4       | 0    | 224   | 902789   | 86%
4/2       | 2    | 434   | 543440   | 51%
4/8       | 4    | 487   | 220349   | 21%
1/2       | 1    | 120   | 138723   | 13%
1/3       | 1    | 128   | 97328    | 9%
2/5       | 0    | 260   | 34234    | 3%
2/6       | 0    | 268   | 11723    | 1%
```

Follow this example to display a summary of traffic management VOQ maximum buffer utilization for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 max-buffer-util
```

```
----- Ports 1/1 - 1/36 -----
Max Buffer Size | Max Buffer Util
-----|-----
6007013804 | 96%
```

Follow this example to display a summary of traffic management VOQ discards for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 discards
```

```
----- Ports 1/1 - 1/36 -----
Dest Port | Prio | Queue | Discards
-----|-----|-----|-----
3/1       | 0    | 320   | 2473804
2/4       | 0    | 224   | 1867789
4/2       | 2    | 434   | 1023452
4/8       | 4    | 487   | 920349
1/2       | 1    | 120   | 858723
1/3       | 1    | 128   | 75328
2/5       | 0    | 260   | 22234
2/6       | 0    | 268   | 5248
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show tm voq-stat slot

Displays the traffic management VOQ statistics for a line card (LC) in a named slot.

## Syntax

```
show tm voq-stat slot slot_number [ cpu-group [ cpu_group_id | all ]
```

## Parameters

*slot\_number*

The LC slot.

**cpu-group** *cpu\_group\_id*

The ID number for the CPU group.

## Modes

Privileged EXEC mode.

## Examples

To display information about the VOQ for the LC in slot 1 CPU group 1 use the following command.

```
device# show tm voq-stat slot 1 cpu-group 1
CPU Group 1 Prio 0
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0

CPU Group 1 Prio 1
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0

CPU Group 1 Prio 2
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0

CPU Group 1 Prio 3
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0

CPU Group 1 Prio 4
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0

CPU Group 1 Prio 5
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0

CPU Group 1 Prio 6
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0

CPU Group 1 Prio 7
  EnQue Pkt Count          100
  EnQue Bytes Count       22400
  Total Discard Pkt Count    0
  Total Discard Bytes Count  0
  Current Queue Depth      0
  Maximum Queue Depth since last read 0
```

show tm voq-stat slot

## History

Release version	Command history
16r.1.00	This command was introduced.

# show topology-group

Displays topology group information.

## Syntax

```
show topology-group [ group-id ]
```

## Parameters

*group-id*

Displays the information of the topology group of the specified ID.

## Modes

User EXEC mode

Privileged EXEC mode

Global configuration mode

Interface configuration mode

VLAN configuration mode

## Usage Guidelines

## Command Output

The **show topology-group** command displays the following information:

Output field	Description
master-vlan	The master VLAN for the topology group. The settings for STP, MRP, or VSRP on the control ports in the master VLAN apply to all control ports in the member VLANs within the topology group.
member-vlan	The member VLANs in the topology group.
Common control ports	The master VLAN ports that are configured with Layer 2 protocol information. The Layer 2 protocol configuration and state of these ports in the master VLAN applies to the same port numbers in all the member VLANs.
Per vlan free ports	The ports that are not controlled by the Layer 2 protocol information in the master VLAN.

## Examples

The following example displays the topology group information.

```
device# show topology-group
Topology Group 3
=====
master-vlan 2
member-vlan none
Common control ports      L2 protocol
ethernet 1/1/1            MRP
ethernet 1/1/2            MRP
ethernet 1/1/5            VSRP
ethernet 1/2/22           VSRP
Per vlan free ports
ethernet 1/2/3            Vlan 2
ethernet 1/1/4            Vlan 2
ethernet 1/2/11           Vlan 2
ethernet 1/2/12           Vlan 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show tunnel

Displays information pertaining to a tunnel interface.

## Syntax

```
show tunnel tunnel-id
```

## Parameters

*tunnel-id*

Specifies the tunnel ID.

## Modes

Privileged EXEC Mode

## Examples

This example displays tunnel information.

```
device# show tunnel 10
Tunnel 10, mode GRE
Ifindex 0x7c40000a, Admin state up, Oper state up
Source IP 14.101.0.4, Vrf default-vrf
Destination IP 15.10.0.3
Tunnel IP Interface : Ve 501 up
Tunnel TTL 255      Tunnel DSCP 0
Tunnel QosMode PIPE
Keepalive Interval 10000  RetryCount 3 TimeRemaining 27861 msec
GRE Keep Alive : RX 62      TX 62

Active next hops:
IP: 13.10.0.3, Vrf: default-vrf
Egress L3 port: Ve 10, Outer SMAC: 609c.9f0d.4a14
Outer DMAC: 001b.ed9f.1700
Egress L2 Port: Unknown, Outer ctag: 0, stag:0, Egress mode: Local
BUM forwarder: no
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show tunnel statistics

Displays tunnel statistics.

## Syntax

```
show tunnel statistics tunnel-id mode [ gre ]
```

## Parameters

*tunnel-id*

Filters by the tunnel ID.

**mode**

Filters by tunnel mode.

**gre**

Specifies GRE tunnels.

## Modes

Privileged EXEC Mode

## Examples

This example displays tunnel statistics filtered by the tunnel ID.

```
device# show tunnel statistics 11
Tnl ID   RX packets   TX packets   RX bytes   TX bytes
-----
11       0             10           (NA)       640
```

This example displays tunnel statistics filtered by tunnel mode.

```
device# show tunnel statistics mode gre
Tnl ID   RX packets   TX packets   RX bytes   TX bytes
-----
10       0             10           (NA)       640
11       0             20           (NA)       1280
12       0             50           (NA)       22000
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# show udld

Shows global UDLD information.

## Syntax

```
show udld
```

## Modes

Privileged EXEC mode

## Usage Guidelines

This command displays global unidirectional link detection (UDLD) protocol configuration values such as whether the protocol is enabled on the switch and the *hello* time and timeout values.

## Examples

The following example displays global UDLD information for the device.

```
device# show udld
UDLD Global Information
  Admin State:      UDLD enabled
  UDLD hello time:  500 milliseconds
  UDLD timeout:    2500 milliseconds
```

# show udd interface

Display unidirectional link detection (UDLD) protocol information for the specified interface.

## Syntax

```
show udd interface [ ethernet slot/port ]
```

## Parameters

### ethernet

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

### slot/port

Specifies a valid slot and port number.

## Modes

Privileged EXEC mode.

## Usage Guidelines

The following describes the values that appear in the output headings for this command.

**TABLE 9** Description UDLD headings

Heading	Description
State	Describes if UDLD is enable or disabled.
Mode	Describes if the mode is Receive, Transmit, or Both (Transmit/Receive).
Advertise Transmitted	Describes how often the advertisement is transmitted.
Hold time for advertise	Describes the hold time for receiving devices before discarding.
Re-init Delay Timer	The timer for the reinitializing delay
Tx Delay Timer	The timer for transmission
DCBX Version	The current DCBX version
Auto-Sense	States whether Auto-Sense is active.
Transmit TLVs	Describes what information is being transmitted for the TLV.
DCBX FCoE Priority Bits	Describes the current FCoE priority bit for DCBX.

## Examples

To display UDLD information for a specific Ethernet interface:

```
device# show udd interface ethernet 2/6
Global Admin State:  UDL enabled

UDLD information for Ethernet 2/6
  UDLD Admin State:      Enabled
  Interface Operational State: Bidirectional link
  Remote hello time:    Unknown
  Remote MAC Addr:      0024.3890.0d81
  Local system id:      0x9f01fee0
  Remote system id:     0x24900c00
  Local port :          2/6
  Remote port :         9/2
  Local link id:        0x0
  Remote link id:       0x0
  Last Xmt Seq Num:    43849
  Last Rcv Seq Num:    43880
```

# show uddl statistics

Shows UDLD statistics.

## Syntax

```
show uddl statistics [ interface [ ethernet slot/port ] ]
```

## Parameters

### ethernet

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

### *slot/port*

Specifies a valid slot and port number.

## Modes

Privileged EXEC mode

## Usage Guidelines

This command displays all unidirectional link detection (UDLD) protocol statistics or shows the statistics on a specified port.

## Examples

To show UDLD statistics on a specific Ethernet interface:

```
device# show uddl statistics interface ethernet 5/1
UDLD Interface statistics for Ethernet 5/1
Frames transmitted: 310
Frames received: 301
Frames discarded: 0
Frames with error: 0
Remote port id changed: 0
Remote MAC address changed: 0
```

# show users

Displays the users logged in to the system and locked user accounts.

## Syntax

```
show users
```

## Modes

Privileged EXEC mode

## Examples

The following example displays active user sessions and locked user accounts.

```
device# show users
**USER SESSIONS**
Username   Role   Host IP   Device   Time Logged In
jsmith     user   192.0.2.0 Cli       2016-04-30 01:59:35
jdoe       admin  192.0.2.1 Cli       2016-05-30 01:57:41

**LOCKED USERS**
testUser
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# show vrrp

Displays information about IPv4 VRRP and VRRP-E sessions.

## Syntax

**show vrrp**

**show vrrp** *VRID* [ **detail** | **summary** ]

**show vrrp detail**

**show vrrp interface** { **ethernet** *slot/port* | **ve** *vlan\_id* } [ **detail** | **summary** ]

**show vrrp summary** [ **vrf** { *vrf-name* | **all** } ]

## Parameters

*VRID*

The virtual group ID about which to display information. The range is from 1 through 16.

**detail**

Displays all session information in detail, including session statistics.

**summary**

Displays session-information summaries.

**interface**

Displays information for an interface that you specify.

**ethernet** *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

**ve** *vlan\_id*

Specifies the VE VLAN number.

**vrf**

Specifies a VRF instance or all VRFs.

*vrf-name*

Specifies a VRF instance. For the default vrf, enter **default-vrf**.

**all**

Specifies all VRFs.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to display information about VRRP and VRRP-E sessions, either in summary or full-detail format. You can also specify a particular virtual group ID or interface for which to display output.

This command is for VRRP and VRRP-E. VRRP-E supports only the VE interface type.

To display information for VRRP sessions using the default VRF, you can use the **show vrrp summary** command syntax (with no additional parameters).

For the default or a named VRF, you can use the **show vrrp summary vrf** command syntax with the *vrf-name* option.

To display information for all VRFs, use the **show vrrp summary vrf all** command.

## Examples

The following example shows all VRRP session information in detail, including session statistics.

```
device# show vrrp detail

Total number of VRRP session(s)   : 2

VRID 14
  Interface: Ve 2018;  Ifindex: 1207961570
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.18.1.100
  Virtual MAC Address: 0000.5e00.0112
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec (default: 1 sec)
  Preempt mode: ENABLE (default: ENABLE)
  Hold time: 0 sec (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                Priority  Port Status
    =====                =====  =====

Global Statistics:
=====
  Checksum Error : 0
  Version Error  : 0
  VRID Invalid   : 0

Session Statistics:
=====
  Advertisements           : Rx: 0, Tx: 49
  Gratuitous ARP           : Tx: 1
  Session becoming master  : 1
  Advts with wrong interval : 0
  Prio Zero pkts          : Rx: 0, Tx: 0
  Invalid Pkts Rvcd       : 0
  Bad Virtual-IP Pkts     : 0
  Invalid Authenticon type : 0
  Invalid TTL Value       : 0
  Invalid Packet Length   : 0

VRID 15
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.19.1.100
  Virtual MAC Address: 0000.5e00.0113
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec (default: 1 sec)
  Preempt mode: ENABLE (default: ENABLE)
  Hold time: 0 sec (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                Priority  Port Status
    =====                =====  =====

Global Statistics:
=====
```



```
Checksum Error : 0
Version Error  : 0
VRID Invalid   : 0
```

Session Statistics:

```
=====
Advertisements      : Rx: 0, Tx: 81
Gratuitous ARP      : Tx: 1
Session becoming master : 1
Advts with wrong interval : 0
Prio Zero pkts      : Rx: 0, Tx: 0
Invalid Pkts Rvcd   : 0
Bad Virtual-IP Pkts : 0
Invalid Authentication type : 0
Invalid TTL Value   : 0
Invalid Packet Length : 0
```

The following example displays summary information for VRRP statistics on the VRF named Marketing.

```
device# show vrrp summary vrf Marketing
```

```
Total number of VRRP session(s) : 1
Master session count : 1
Backup session count : 0
Init session count : 0
```

VRID	Session	Interface	Admin State	Current Priority	State	Short-path Forwarding	Revert Priority	SPF Reverted
14	VRRP	Ve 2018	Enabled	100	Master			

The following example displays summary information for VRRP statistics on all VRFs.

```
device# show vrrp summary vrf all
```

```
Total number of VRRP session(s) : 2
Master session count : 2
Backup session count : 0
Init session count : 0
```

VRID	Session	Interface	Admin State	Current Priority	State	Short-path Forwarding	Revert Priority	SPF Reverted
14	VRRP	Ve 2018	Enabled	100	Master			
15	VRRP	Ve 2019	Enabled	100	Master			

The following example displays summary information for VRRP statistics on the default VRF. (This command is equivalent to **show vrrp summary**.)

```
device# show vrrp summary vrf default-vrf
```

```
Total number of VRRP session(s) : 1
Master session count : 1
Backup session count : 0
Init session count : 0
```

VRID	Session	Interface	Admin State	Current Priority	State	Short-path Forwarding	Revert Priority	SPF Reverted
15	VRRP	Ve 2019	Enabled	100	Master			

The following example displays information for VRRP-E tracked networks.

```

device# show vrrp detail

Total number of VRRP session(s)   : 1

VRID 3
Interface: Ve 100;  Ifindex: 1207959652
Mode: VRRPE
Admin Status: Enabled
Description :
Address family: IPv4
Version: 2
Authentication type: No Authentication
State: Master
Session Master IP Address: Local
Virtual IP(s): 10.1.1.100
Virtual MAC Address: 02e0.523d.750a
Configured Priority: unset (default: 100); Current Priority: 100
Advertisement interval: 1 sec (default: 1 sec)
Preempt mode: DISABLE (default: DISABLED)
Advertise-backup: DISABLE (default: DISABLED)
Backup Advertisement interval: 60 sec (default: 60 sec)
Short-path-forwarding: Disabled
Revert-Priority: unset; SPF Reverted: No
Hold time: 0 sec (default: 0 sec)
Master Down interval: 4 sec
Trackport:
  Port(s)                Priority  Port Status
  =====                =====  =====

Tracknetwork:
  Network(s)             Priority  Status
  =====                =====  =====
  10.20.1.0/24           50      Up

Global Statistics:
=====
Checksum Error : 0
Version Error  : 0
VRID Invalid   : 0

Session Statistics:
=====
Advertisements           : Rx: 0, Tx: 35
Neighbor Advertisements  :           : Tx: 19
Session becoming master  : 1
Advts with wrong interval : 0
Prio Zero pkts           : Rx: 0, Tx: 0
Invalid Pkts Rvcd        : 0
Bad Virtual-IP Pkts      : 0
Invalid Authentication type : 0
Invalid TTL Value        : 0
Invalid Packet Length    : 0
VRRPE backup advt sent   : 0
VRRPE backup advt recvd  : 0

```

## History

Release version	Command history
16r.1.00	This command was introduced.

# Commands Si - Z

---

## snmp-server community

Sets the community string and associates it with the user-defined group name to restrict the access of MIB for SNMPv1 and SNMPv2c requests.

### Syntax

`snmp-server community string [ group group-name ]`

`no snmp-server community string [ group group-name ]`

### Command Default

None

### Parameters

*string*

Specifies the community name string. Enter an alphanumeric string with 2 to 16 characters.

**group** *group-name*

Specifies the group name associated with the community name.

### Modes

Global configuration mode

### Usage Guidelines

Use a **no** form of this command to remove an community string or the group from the community.

The maximum number of SNMP communities supported is 256.

### Examples

The following example adds the community string named public and associates the group name named user with it.

```
device(config)# snmp-server community public groupname user
```

### History

Release version	Command history
16r. 1.00	This command was introduced.

# snmp-server contact

Sets the SNMP server contact string.

## Syntax

```
snmp-server contact string [ location string ] [ sys-descr string ]  
no snmp-server contact string [ location string ] [ sys-descr string ]
```

## Command Default

The default contact string is BrocadeCommunicationSystem.

The default location string is BrocadeTcsHyd.

The default system description string is BrocadeSupport.

## Parameters

*string*

Specifies the server contact. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

**location** *string*

Specifies the SNMP server location string. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

**sys-descr** *string*

Specifies the Management Information Base (MIB-2) object identifier (OID) system description. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

## Modes

Global configuration mode

## Usage Guidelines

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

## Examples

The following example sets the SNMP server contact string to "Operator 12345".

```
device(config)# snmp-server contact "Operator 12345"
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# snmp-server context

Maps the context name in an SNMPv3 packet protocol data unit (PDU) to the name of a VPN routing and forwarding (VRF) instance.

## Syntax

```
snmp-server context context_name [ vrf-name vrf_name ]
no snmp-server context context_name [ vrf-name vrf_name ]
```

## Command Default

None

## Parameters

*context\_name*

Specifies the context name that is passed in the SNMP PDU.

**vrf-name** *vrf\_name*

Specifies the VRF instance that can be retrieved when an SNMP request is sent with the context name.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no** form of the command to delete the SNMP server context.

For SNMPv1 and SNMPv2, you must map the context with the community string. The SNMP agent supports 256 contexts to support context-to-VRF mapping.

For SNMPv3, you only need to map the context with the VRF. The SNMPv3 request PDU itself provisions for the context. Only one context is allowed for each VRF instance.

### ATTENTION

SNMP SET requests work only on the default VRF.

## Examples

The following example configures an SNMP server context to a VRF for SNMPv1 or SNMPv2.

```
device# configure terminal
device(config)# snmp-server community public groupname admin
device(config)# snmp-server context mycontext vrf myvrf
device(config)# snmp-server mib community-map public context mycontext
```

The following example configures an SNMP server context to a VRF for SNMPv3.

```
device# configure terminal
device(config)# snmp-server context mycontext1 vrf myvrf1
```

## History

Release version	Command history
16r.1.00	This command was introduced.
16r.1.01	This command was modified to update the Usage Guidelines related to SNMP SET requests.

# snmp-server enable trap

Enables the SNMP traps.

## Syntax

`snmp-server enable trap`

`no snmp-server enable trap`

## Command Default

The SNMP server traps are enabled by default.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no** form of this command to disable the SNMP traps.

## Examples

The following example disables the SNMP traps.

```
device# configure terminal
device(config)# no snmp-server enable trap
```

The following example enables the SNMP traps.

```
device# configure terminal
device(config)# snmp-server enable trap
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# snmp-server engineid local

Configures an SNMP engine ID for the SNMP agent.

## Syntax

```
snmp-server engineid local engine_id
no snmp-server engineid local
```

## Command Default

A default engine ID is generated during system start up.

## Modes

Global configuration mode

## Usage Guidelines

A reboot is necessary for the configured engine ID to become active.

Use the **no** form of the command to remove the configured engine ID from database.

## Examples

The following example configures an engine ID for the SNMP agent.

```
device(config)# snmp-server engineid local 10:00:00:05:33:51:A8:65:05:33:51:A8
```

The following example removes the configured engine ID from the database.

```
device(config)# no snmp-server engineid local
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## snmp-server group

Creates user-defined groups for SNMPv1/v2/v3 and configures read, write, and notify permissions to access the MIB view.

### Syntax

```
snmp-server group groupname { v1 | v2c | v3 { auth | noauth | priv } } [ read viewname ] [ write viewname ] [ notify viewname ]
```

```
no snmp-server group groupname { v1 | v2c | v3 { auth | noauth | priv } } [ read viewname ] [ write viewname ] [ notify viewname ]
```

### Command Default

None

### Parameters

*groupname*

Specifies the name of the SNMP group to be created.

**v1 | v2c | v3**

Specifies the version of SNMP.

**auth | noauth | priv**

Specifies the various security levels for SNMPv3.

**auth**

Specifies the authNoPriv security level. Password authentication is used based on either MD5 or SHA hash authentication and no encryption is used for communications between the devices.

**noauth**

Specifies the noAuthNoPriv security level. If no security level is specified, noauth is the default. This security level means that there is no authentication password exchanged and the communications between the agent and the server are not encrypted. The SNMP requests are authorized based on a username string match similar to the community string for SNMPv1/v2c.

**priv**

Specifies the authPriv security level. Password authentication is used based on either MD5 or SHA hash authentication and the communication between the agent and the server are also encrypted.

**read** *viewname*

Specifies the name of the view that enables you to provide read access.

**write** *viewname*

Specifies the name of the view that enables you to provide both read and write access.

**notify** *viewname*

Specifies the name of the view that enables you to provide access to the MIB for trap or inform.

## Modes

Global configuration mode

## Usage Guidelines

Maximum number of SNMP groups supported is 10.

## Examples

The following example creates SNMP server group entries for SNMPv3 user group with auth or noauth permission.

```
device(config)# snmp-server group group1 v3 auth read myview write myview notify myview
device(config)# snmp-server group group2 v3 noauth read all write all notify all
device(config)# snmp-server group group3 v3 auth
```

The following example removes the configured SNMP server groups.

```
device(config)# no snmp-server group test1 v3 auth
device(config)# no snmp-server group TEST1 v3 auth read myview write myview
device(config)# no snmp-server group TEST2 v3 noauth read all write all notify all
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# snmp-server host

Configures the SNMP trap server host attributes.

## Syntax

```
snmp-server host { ipv4_host | ipv6_host | dns_host } community_string [ version { 1 | 2c } ] [ udp-port port ] [ severity-level |
  { none | debug | info | warning | error | critical } ] [ use-vrf vrf-name ]
```

```
no snmp-server host { ipv4_host | ipv6_host | dns_host } community_string [ version { 1 | 2c } ] [ udp-port port ] [ severity-
  level | { none | debug | info | warning | error | critical } ] [ use-vrf vrf-name]
```

## Parameters

**host** { *ipv4\_host* | *ipv6\_host* | *dns\_host* }

Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

*community\_string*

Specifies the community string associated with the host entry. The number of characters available for the string ranges from 1 through 64.

**version** { *1* | *2c* }

Selects version 1 or 2c traps to be sent to the specified trap host.

**udp-port** *port*

Specifies the UDP port where SNMP traps will be received. Valid port IDs range from 0 through 65535. The default port is 162.

**severity-level** { *none* | *debug* | *info* | *warning* | *error* | *critical* }

Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of **none** is specified, all traps are filtered and no RASLog traps are received.

**use-vrf** *vrf-name*

Specifies a VRF through which to communicate with the SNMP host. By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

## Modes

Global configuration mode

## Usage Guidelines

This command sets the trap destination IP addresses and SNMP version, associates a community string with a trap host community string (for v1 and v2c), and specifies the UDP destination port where SNMP traps will be received.

To configure SNMP trap hosts associated with community strings, you must create the community string using the **snmp-server community** command before configuring the host.

The host supports six communities and their associated trap recipients and trap recipient severity levels. The default value for the trap recipient of each community is 0.0.0.0. The length of the community string should be between 2 and 64 characters.

The `no snmp-server host host community-string string version 2c` command brings version 2c down to version 1.

The `no snmp-server host host community-string string` command removes the SNMP server host from the device configuration altogether.

## Examples

The following example creates an entry for trap host 1050:0:0:0:5:600:300c:326b associated with community "public." The trap host receives traps from the configured device.

```
device(config)# snmp-server host 1050:0:0:0:5:600:300c:326b public severity-level Info
```

The following example creates an entry for trap host brcd.extremenetworks.com associated with community "public." The trap host receives traps from the configured device.

```
device(config)# snmp-server host brcd1.extremenetworks.com public severity-level info
```

The following example associates "commaccess" as a read-only community and set 10.32.147.6 as a trap recipient with SNMP version 2c on target port 162.

```
device(config)# snmp-server host 10.32.147.6 commaccess version 2c udp-port 162
```

The following example creates a trap host (10.23.23.45) associated with the community "public", which will receive all traps with the severity level of Info.

```
device(config)# snmp-server host 10.23.23.45 public severity-level info
```

The following example resets the severity level to None.

```
device(config)# snmp-server host 10.23.23.45 public severity-level none
```

The following example specifies a VRF to communicate with the host.

```
device(config)# snmp-server host 10.24.61.10 public use-vrf myvrf
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# snmp-server location

Sets the SNMP server location string.

## Syntax

```
snmp-server location string [ contact string ] [ sys-descr string ]  
no snmp-server location string [ contact string ] [ sys-descr string ]
```

## Command Default

The default location string is BrocadeTcsHyd.

The default contact string is BrocadeCommunicationSystem.

The default system description string is BrocadeSupport.

## Parameters

### **location** *string*

Specifies the SNMP server location string. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

### **contact** *string*

Specifies the server contact. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

### **sys-descr** *string*

Specifies the Management Information Base (MIB-2) object identifier (OID) system description. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

## Modes

Global configuration mode

## Usage Guidelines

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

## Examples

The following example sets the SNMP server location string to "Building 3 Room 214".

```
device(config)# snmp-server location "Building 3 Room 214"
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# snmp-server mib community-map

Maps an SNMP community string to an SNMP context.

## Syntax

```
snmp-server mib community-map community-name context context-name  
no snmp-server mib community-map community-name context context-name
```

## Command Default

None

## Parameters

*community-name*  
Specifies an SNMP community name.

**context** *context-name*  
Specifies an SNMP context.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no** form of this command to remove a community string and its associated context name.

Any incoming SNMPv1/v2c requests with the specified community name uses the context name specified by this command. The context name can be used in SNMP requests for "ipCidrRouteTable." One community can be mapped to only one context. However, a single context can be mapped to multiple communities.

Before mapping the community to context, a valid context should be configured by using the **snmp-server context** command and a valid community string should be configured by using the **snmp-server community** command.

## Examples

The following example maps an SNMP community string to a context name.

```
device# configure terminal  
device(config)# snmp-server mib community-map public context mycontext
```

The following example removes an SNMP community string and its associated context name.

```
device(config)# no snmp-server mib community-map public context mycontext
```



## History

Release version	Command history
16r.1.00	This command was introduced.

# snmp-server sys-descr

Sets the Management Information Base (MIB-2) object identifier (OID) system description.

## Syntax

```
snmp-server sys-descr string [ contact string ] [ location string ]
```

```
no snmp-server sys-descr string [ contact string ] [ location string ]
```

## Command Default

The default system description string is BrocadeSupport.

The default contact string is BrocadeCommunicationSystem.

The default location string is BrocadeTcsHyd.

## Parameters

*string*

Specifies the system description. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

**contact** *string*

Specifies the server contact. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

**location** *string*

Specifies the SNMP server location string. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

## Modes

Global configuration mode

## Usage Guidelines

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

## Examples

The following example sets the system description OID to "Extreme Cluster device".

```
device(config)# snmp-server sys-descr "Extreme Cluster device"
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## snmp-server user

Creates or changes the attributes of SNMPv3 users, and allows the SNMPv3 user to be associated with the user-defined group name.

### Syntax

```
snmp-server user username [ groupname group-name ] [ auth { md5 | sha | noauth } ] [ auth-password string [ encrypted ] ]
  [ priv { DES | AES128 | nopriv } ] [ priv-password string [ encrypted ] ]
```

```
no snmp-server user username [ groupname group-name ] [ auth { md5 | sha | noauth } ] [ auth-password string
  [ encrypted ] ] [ priv { DES | AES128 | nopriv } ] [ priv-password string [ encrypted ] ]
```

### Command Default

None

### Parameters

#### *username*

The name of the user that connects to the agent. The name must be between 1 and 16 characters long.

#### **groupname** *group-name*

The name of the group to which the user is associated. The configured user is allowed to be associated with the user-defined groups created using the **snmp-server group** command.

#### **auth**

Initiates an authentication level setting session. The default level is **noauth**.

#### **noauth**

Specifies "No Authentication Protocol".

#### **md5**

The HMAC-MD5-96 authentication level.

#### **sha**

The HMAC-SHA-96 authentication level.

#### **auth-password** *string*

A string that enables the agent to receive packets from the host. Passwords are plain text and must be added each time for each configuration replay. The password must be between 1 and 32 characters long.

#### **priv**

Initiates a privacy authentication level setting session. The default level is **nopriv**.

#### **DES**

Specifies the DES privacy protocol.

#### **AES128**

Specifies the AES128 privacy protocol.

#### **nopriv**

Specifies "No Privacy Protocol".

**priv-password** *string*

Specifies a string (not to exceed 32 characters) that enables the host to encrypt the contents of the message that it sends to the agent. Passwords are plain text and must be added each time for each configuration replay. The privacy password alone cannot be configured. You configure the privacy password with the authentication password.

**encrypted**

Encrypts the input for auth/priv passwords. The encrypted key should be used only while entering the encrypted auth/priv passwords.

## Modes

Global configuration mode

## Usage Guidelines

This command configures SNMPv3 users that can be associated with a trap and inform response functionality. This command also allows configured user to be associated with user-defined SNMP groups created using the **snmp-server group** command. The maximum number of SNMP users that can be configured is 10. Optional encryption for **auth-password** and **priv-password** is also provided.

When creating a new SNMPv3 user without group name, by default there is no group name mapped with the SNMPv3 user. You must map the configured SNMPv3 user with any non-existing or existing group name available in the group CLI configuration to contact the device through SNMPv3.

This command may not be successful where encrypted passwords are generated by third-party or open-source tools.

Use a **no** form of this command to do one of more of the following:

- Remove the specified user and all entities associated with it
- Remove the groupname from the user

## Examples

The following example configures a basic authentication policy.

```
device(config)# snmp-server user extreme groupname snmpadmin auth md5 auth-password user123 priv AES128
priv-password user456
```

The following example configures plain-text passwords.

```
device(config)# snmp-server user snmpadmin1 auth md5 auth-password private123 priv DES priv-password
public123
```

The following example configures encrypted passwords.

```
device(config)# snmp-server user snmpadmin2 groupname snmpadmin auth md5 auth-password "MVb
+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted
```

The following example creates the SNMP users "user1" and "user2" associated with user-defined group "group1" under global configuration mode.

```
device(config)# snmp-server user user1 groupname group1
device(config)# snmp-server user user2 groupname group1 auth md5 auth-password password priv DES priv-
password password
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# snmp-server v3host

Specifies the host recipient for SNMPv3 trap notification.

## Syntax

```
snmp-server v3host { ipv4_host | ipv6_host | dns_host } user_name [ notifytype { traps | informs } ] [ engineid engine-id ]
[ udp-port port_number ] [ severity-level | { none | debug | info | warning | error | critical } ] [ use-vrf { vrf-name } ]
```

```
no snmp-server v3host { ipv4_host | ipv6_host | dns_host } user_name [ notifytype {traps | informs}] [ engineid engine-id ]
[ udp-port port_number ] [ severity-level | {none | debug | info | warning | error | critical } ] [ use-vrf ]
```

## Parameters

**ipv4\_host | ipv6\_host | dns\_host**

Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

*user\_name*

Specifies the SNMPv3 user name to be associated with the SNMPv3 host entry.

**notifytype traps | informs**

Specifies the type of notification traps that are sent for the host. Traps and informs are supported. The default notify type is traps.

**engineID engine-id**

Configures the remote engine ID to receive informs on a remote host.

**udp-port port\_number**

Specifies the UDP port of the host. The default UDP port number is 162.

**severity-level { none | debug | info | warning | error | critical }**

Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of None is specified, all traps are filtered and no RASLog traps are received. The default severity level is none.

**use-vrf vrf-name**

Configures SNMP to use the specified VRF to communicate with the host. The default is mgmt-vrf.

## Modes

Global configuration mode

## Usage Guidelines

You can associate a global SNMPv3 host only with global SNMPv3 users and the local SNMPv3 host only with local SNMPv3 users. You cannot create a SNMPv3 host by associating with the local SNMPv3 users and vice versa.

## Examples

The following example creates an entry for SNMPv3 trap IPv4 host 10.23.23.45 associated with SNMP user "snmpadmin1."

```
device(config)# snmp-server v3host 10.23.23.45 snmpadmin1 severity-level info
```

The following example creates an entry for SNMPv3 trap IPv6 host 1050:0:0:0:5:600:300c:326b associated with SNMP user "snmpadmin2." The trap host receives SNMPv3 traps from the configured device.

```
device(config)# snmp-server v3host 1050::5:600:300c:326b snmpadmin2 severity-level Info
```

The following example associates the default-vrf VRF for a trap host recipient.

```
device(config)# snmp-server v3host 10.24.61.10 public use-vrf default-vrf
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# snmp-server view

Creates a view entry with MIB object IDs to be included or excluded for user access.

## Syntax

**snmp-server view** *view-name* *mib\_tree* **included** | **excluded**

**no snmp-server view** *view-name* *mib\_tree* **included** | **excluded**

## Command Default

None

## Parameters

*view-name*

Specifies the alphanumeric name to identify the view. The name should not contain spaces.

*mib\_tree*

Specifies the MIB object ID called Object Identifiers (OIDs) that represent the position of the object or sub-tree in the MIB hierarchy.

**included** | **excluded**

Specifies whether the specified MIB object ID must be included in the view or excluded from the view.

## Modes

Global configuration mode

## Usage Guidelines

The maximum number of views supported with MIB tree entries is 10. Either a single view name associated with 10 different MIB object IDs or 10 different view names associated with each one of the MIB object IDs is allowed.

## Examples

The following example creates an SNMP view entry "view1" with excluded permission for the MIB object ID "1.3.6.1.2.1.1.3":

```
device(config)# snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

The following example creates an SNMP view entry "view2" with included permission for the MIB object ID "1.3.6.1.":

```
device(config)# snmp-server view view2 1.3.6.1 included
```

The following example removes the SNMP view entry "view1" from the configuration list.

```
device(config)# no snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# soft-preemption

The **soft-preemption** command enables soft preemption functionality. This command must be used on both the primary and secondary paths.

## Syntax

```
soft-preemption
no soft-preemption
```

## Command Default

The soft-preemption function is disabled.

## Modes

MPLS LSP configuration mode.

## Usage Guidelines

The **no** function disables soft preemption for the path on which the command is executed.

## Examples

The following example shows how configure a primary path.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp test
device(config-router-mpls-lsp-test)# soft-preemption
```

The following example shows how to configure a secondary path.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp test
device(config-router-mpls-lsp-test)# secpath sec
device(config-router-mpls-lsp-test-secpath-sec)# soft-preemption
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# soft-preemption cleanup-timer

Sets the amount of time that the point of preemption must wait to receive the path tear notification from the ingress LSR before sending a hard preemption path error.

## Syntax

```
soft-preemption { cleanup-timer | value }
no soft-preemption { cleanup-timer | value }
```

## Command Default

The soft-preemption cleanup-timer is disabled on the router.

## Parameters

**cleanup-timer** *value*

The *value* is the time the point of preemption must wait to receive the path tear notification from the ingress LSR, before sending a hard preemption path error. Values ranging from 1 - 29 are not valid values for this timer. The default setting is 30 seconds. The acceptable range for this timer is 30 - 300. A value of 0 indicates soft preemption is disabled on the router.

## Modes

MPLS policy mode.

## Usage Guidelines

The **no** function returns the timer value settings to the default setting (30 seconds).

## Examples

The following example configures the soft-preemption cleanup-timer to 30 seconds, which is the default setting.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# soft-preemption cleanup-timer 30
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# source

Configures the source address or a source interface for a tunnel interface.

## Syntax

```
source { ip-address | ethernet slot/port | loopback number | ve vlan_id }  
no source
```

## Command Default

No source address or interface is configured.

## Parameters

*ip-address*  
Specifies the IPv4 address of an interface.

**ethernet** *slot/port*  
Specifies an Ethernet interface.

**loopback** *number*  
Specifies a loopback port.

**ve** *vlan\_id*  
Specifies a VE interface.

## Modes

Interface tunnel configuration mode

## Usage Guidelines

The maximum number of tunnel source supported is 16.

Use the **no source** command to remove the configured source for the tunnel interface.

The tunnel source address should be one of the router IP addresses configured on a physical, loopback, or VE interface, through which the other end of the tunnel is reachable. The source interface must have at least one IP address configured on it.

When the physical/ve interface is specified as the source of the GRE tunnel, the lowest IP address of that interface is used as the tunnel source IP address. If the smallest IP address is removed from the interface, the next smallest IP address is used as the tunnel source.

## Examples

This example configures the source address for the tunnel interface.

```
device# configure terminal  
device(config)# interface tunnel 5  
device(config-intf-tunnel-5)# source 10.1.2.4
```

This example sets an Ethernet interface as a source tunnel.

```
device# configure terminal
device(config)# interface tunnel 3
device(config-intf-tunnel-3)# source ethernet 3/1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree autoedge

Enables automatic edge detection.

## Syntax

`spanning-tree autoedge`

`no spanning-tree autoedge`

## Command Default

Auto detection is not enabled.

## Modes

Interface configuration mode

## Usage Guidelines

The port can become an edge port if no Bridge Protocol Data Unit (BPDU) is received.

## Examples

To enable automatic edge detection:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree autoedge
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree bpdu-mac

Sets the MAC address of the Bridge Protocol Data Unit (BPDU).

## Syntax

```
spanning-tree bpdu-mac [ 0100.0ccc.cccd | 0304.0800.0700 ]
no spanning-tree bpdu-mac [ 0100.0ccc.cccd | 0304.0800.0700 ]
```

## Parameters

```
0100.0ccc.cccd
    Cisco Control Mac
0304.0800.0700
    Extreme Control Mac
```

## Modes

Interface configuration mode

## Usage Guidelines

This command will only take effect when the protocol is PVST+ or R-PVST+.

Extreme devices support PVST+ and R-PVST+ only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Enter **no spanning-tree bpdu-mac 0100.0ccc.cccd** to remove the address.

## Examples

To set the MAC address of the BPDU:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# spanning-tree cost

Changes an interface's spanning-tree port path cost.

## Syntax

**spanning-tree cost** *cost*

**no spanning-tree cost** *cost*

## Command Default

The default path cost is 200000000.

## Parameters

*cost*

Specifies the path cost for the Spanning Tree Protocol (STP) calculations. Valid values range from 1 through 200000000.

## Modes

Interface configuration mode

## Usage Guidelines

Lower path cost indicates a greater chance of becoming root.

## Examples

To set the port cost to 128:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree cost 128
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree edgeport

Enables the edge port on an interface to allow the interface to quickly transition to the forwarding state.

## Syntax

```
spanning-tree edgeport [ bpdu-guard ]
no spanning-tree edgeport [ bpdu-guard ]
```

## Command Default

Edge port is disabled.

## Parameters

**bpdu-guard**  
Guards the port against the reception of BPDUs.

## Modes

Interface subtype configuration mode

## Usage Guidelines

This command is only for RSTP and MSTP. Use the **spanning-tree portfast** command for STP.

Note the following details about edge ports and their behavior:

- A port can become an edge port if no BPDU is received.
- A port must become an edge port before it receives a BPDU.
- When an edge port receives a BPDU, it becomes a normal spanning-tree port and is no longer an edge port.
- Because ports directly connected to end stations cannot create bridging loops in the network, edge ports directly transition to the forwarding state, and skip the listening and learning states.

## Examples

To enable a port to quickly transition to the forwarding state:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree edgeport
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree edgeport
device(conf-if-eth-1/5)# spanning-tree edgeport bpdu-guard
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree guard root

Enables the guard root to restrict which interface is allowed to be the spanning tree root port or the device's path-to-the-root.

## Syntax

```
spanning-tree guard root [ vlan vlan_id ]
no spanning-tree guard root
```

## Command Default

Guard root is disabled.

## Parameters

**vlan *vlan\_id***  
Specifies a VLAN.

## Modes

Interface configuration mode

## Usage Guidelines

Guard root protects the root bridge from malicious attacks and unintentional misconfigurations where a bridge device that is not intended to be the root bridge becomes the root bridge. This causes severe bottlenecks in the data path. Guard root ensures that the port on which it is enabled is a designated port. If the guard root enabled port receives a superior Bridge Protocol Data Unit (BPDU), it goes to a discarding state.

If the VLAN parameter is not provided, the guard root functionality is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

The root port provides the best path from the switch to the root switch.

## Examples

To enable guard root:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree guard root
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree link-type

Enables and disables the rapid transition for the Spanning Tree Protocol (STP).

## Syntax

```
spanning-tree link-type [ point-to-point | shared ]
```

## Command Default

The `spanning-tree link-type` is set to `point-to-point`.

## Parameters

### `point-to-point`

Enables rapid transition.

### `shared`

Disables rapid transition.

## Modes

Interface subtype configuration mode

## Usage Guidelines

This command overrides the default setting of the link type.

## Examples

To specify the link type as shared:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree link-type shared
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree portfast

Enables the Port Fast feature on an interface to allow the interface to quickly transition to forwarding state.

## Syntax

```
spanning-tree portfast [ bpdu-guard ]
no spanning-tree portfast [ bpdu-guard ]
```

## Command Default

Port Fast is disabled.

## Parameters

**bpdu-guard**  
Guards the port against the reception of BPDUs.

## Modes

Interface subtype configuration mode

## Usage Guidelines

This command is applicable the only for the Spanning Tree Protocol (STP). Port Fast immediately puts the interface into the forwarding state without having to wait for the standard forward time. Use the **spanning-tree edgeport** command for MSTP and RSTP.

BPDU guard disables all portfast-enabled ports should they ever receive BPDU frames. It does not prevent transmitting of BPDU frames.

If you enable **spanning-tree portfast bpdu-guard** on an interface and the interface receives a BPDU, the software disables the interface and puts the interface in the ERR\_DISABLE state.

Enable Port Fast on ports connected to host. Enabling Port Fast on interfaces connected to switches, bridges, hubs, and so on can cause temporary bridging loops, in both trunking and nontrunking mode.

## Examples

To enable a port to quickly transition to the forwarding state:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree portfast
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree portfast
device(conf-if-eth-1/5)# spanning-tree portfast bpdu-guard
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree priority

Changes an interface's spanning-tree port priority.

## Syntax

`spanning-tree priority priority`

`no spanning-tree priority`

## Command Default

The default value is 128.

## Parameters

*priority*

Specifies the interface priority for the spanning tree. The range of valid values is from 0 through 240. Port priority is in increments of 16.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Enter `no spanning-tree priority` to return to the default setting.

## Examples

To configure the port priority to 16:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree priority 16
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# spanning-tree restricted-role

Restricts the role of the port from becoming a root port.

## Syntax

```
spanning-tree restricted-role  
no spanning-tree restricted-role
```

## Command Default

The restricted role is disabled.

## Modes

Interface configuration mode

## Usage Guidelines

Enter **no spanning-tree restricted-role** to return to the default setting.

## Examples

To configure the port from becoming a root port:

```
device# configure terminal  
device(config)# interface ethernet 1/5  
device(conf-if-eth-1/5)# spanning-tree restricted-role
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree restricted-tcn

Restricts the Topology Change Notification (TCN) Bridge Protocol Data Units (BPDUs) sent on the port.

## Syntax

```
spanning-tree restricted-tcn
```

```
no spanning-tree restricted-tcn
```

## Command Default

The restricted TCN is disabled.

## Modes

Interface configuration mode

## Usage Guidelines

Enter **no spanning-tree restricted-tcn** to disable this parameter.

## Examples

To restrict the TCN on a specific interface:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree restricted-tcn
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spanning-tree shutdown

Enables or disables spanning tree on the interface or VLAN.

## Syntax

**spanning-tree shutdown**

**no spanning-tree shutdown**

## Command Default

Spanning tree is disabled by default.

## Modes

Interface (Ethernet or VLAN) configuration mode

## Usage Guidelines

Enter **no spanning-tree shutdown** to enable spanning tree on the interface or VLAN.

Once all of the interfaces have been configured for a VLAN, you can enable Spanning Tree Protocol (STP) for all members of the VLAN with a single command. Whichever protocol is currently selected is used by the VLAN. Only one type of STP can be active at a time.

A physical interface (port) can be a member of multiple VLANs. For example, a physical port can be a member of VLAN 1002 and VLAN 55 simultaneously. In addition, VLAN 1002 can have STP enabled and VLAN 55 can have STP disabled simultaneously.

Vlan 1002 can not be enabled with the **spanning-tree shutdown** command.

## Examples

To disable spanning tree on a specific interface:

```
device# configure terminal
device(config)# interface tengigabitethernet 0/1
device(conf-if-te-0/1)# spanning-tree shutdown
```

To disable spanning tree on a specific interface:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# speed (Ethernet)

Sets the speed negotiation value on an Ethernet interface.

## Syntax

```
speed { 100 | 1000 | 1000-auto | 10000 | auto }
```

## Command Default

The speed is set to **auto**.

## Parameters

**100**

Forces the speed to 100 Mbps.

**1000**

Forces the speed to 1 Gbps.

**1000-auto**

Forces the speed to 1 Gbps AN (802.3 Clause 37 Auto-Negotiation)

**10000**

Forces the speed to 10 Gbps.

**auto**

Allows the interface to negotiate the speed setting.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Use the **auto** keyword to reset the default setting.

Only the SLX 9850 72X10G line card supports 10G/1G auto negotiation and auto detection mode.

## Examples

The following example changes the speed to 1G with auto negotiation.

```
device# configure terminal
device(config)# interface Ethernet 2/1
device(config-if-eth-2/1)# speed 1000-auto
device(config-if-eth-2/1)# no shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spf-interval

Changes the shortest path first (SPF) interval.

## Syntax

```
spf-interval { level-1 | level-2 } max-wait initial-wait second-wait
no spf-interval
```

## Parameters

### level-1

Specifies Level 1 packets only.

### level-2

Specifies Level 2 packets only.

### max-wait

Specifies the maximum interval between SPF recalculations in seconds. The range is from 0 through 120 seconds. The default is 5 seconds.

### initial-wait

Specifies the initial SPF calculation delay in milliseconds after an LSP change. The range is from 0 through 120000 milliseconds. The default is 5000 milliseconds (5 seconds).

### second-wait

Indicates the hold time between the first and second SPF calculations in milliseconds. The range is from 1 through 120000 milliseconds. The default is 5000 milliseconds (5 seconds).

## Modes

IS-IS router configuration mode

## Usage Guidelines

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

## Examples

The following example specifies that the maximum interval in seconds between SPF recalculations is 15 seconds for Level 1 packets. The initial SPF calculation delay is 10000 milliseconds, and the hold time between the first and second SPF calculations is 15000 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# spf-interval level-1 15 10000 15000
```

The following example restores the defaults.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no spf-interval
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# spt-threshold

Sets the threshold for switching to the shortest-path-tree.

## Syntax

```
spt-threshold { rangeseconds | infinity }
no spt-threshold
```

## Command Default

The default is 1 second.

## Parameters

- range**  
Specifies the traffic rate in frames per second. The range is 1 through 4294967295.
- infinity**  
Causes all sources to use the shared RP tree.

## Modes

Router PIM configuration mode.

## Usage Guidelines

## Examples

The following example specifies the traffic rate.

```
device(config)# router pim
device(config-pim-router)# spt-threshold 4294967
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ssh

Connects to a remote server by means of the Secure Shell (SSH) protocol.

## Syntax

```
ssh { IP_address | hostname } [ -c | -l | -m | interface { <N>gigabitethernet | management | ve vlan-id } | vrf vrf-name ] }
```

## Command Default

SSH connects to port 22.

## Parameters

*IP\_address*

Specifies the server IP address in IPv4 or IPv6 format.

*hostname*

Specifies the host name, a string from 1 through 253 characters.

**-c**

Specifies the encryption algorithm for the SSH session. This parameter is optional; if no encryption algorithm is specified, the default (**3des**) is used. Supported algorithms include the following:

**3des**

Triple Data Encryption Standard (DES). This is the default setting.

**aes128-cbc**

AES 128-bits

**aes192-cbc**

AES 192-bits

**aes256-cbc**

AES 256-bits

**-l** *username*

Login name for the remote server. This parameter is optional. If you specify a user name, you will be prompted for a password. If you do not specify a user name, the command assumes you are logging in as root and will prompt for the root password.

**-m**

Specifies the HMAC (Hash-based Message Authentication Code) message encryption algorithm. This parameter is optional; if no encryption algorithm is specified, the default (**hmac-md5**) is used. Supported algorithms include the following:

**hmac-md5**

MD5 128-bits. This is the default setting.

**hmac-md5-96**

MD5 96-bits

**hmac-sha1**

SHA1 160-bits

**hmac-sha1-96**  
SHA1 96-bits

### interface

Specifies an interface.

**<N> gigabitethernet**

Represents a valid, physical Ethernet subtype for all available Ethernet speeds. Enter ? to see which interface subtypes are available. Replace **<N>gigabitethernet** with the desired operand (for example, **tengigabitethernet** specifies a 10-Gb Ethernet port). The use of **gigabitethernet** without a speed value specifies a 1-Gb Ethernet port.

**management**

Specifies a management interface.

**ve** *vlan-id*

Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

**vrf** *vrf-name*

Specifies a VRF instance. See the Usage Guidelines.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to establish an encrypted SSH connection from a switch to a remote networking device. This implementation is based on SSH v2.

To use the **ssh** command on the management VRF, use the **vrf** keyword and enter **mgmt-vrf** manually.

The following features are not supported:

- Displaying SSH sessions
- Deleting stale SSH keys

## Examples

To connect to a remote device using an SSH connection with default settings:

```
device# ssh 10.70.212.152
```

```
The authenticity of host '10.70.212.152 (10.70.212.152)' can't be established.
RSA key fingerprint is f0:2a:7e:48:60:cd:06:3d:f4:44:30:2a:ce:68:fe:1d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.70.212.152' (RSA) to the list of known hosts.
Password:
```

To connect to a remote device using an SSH connection with the management VRF:

```
device# ssh 10.70.212.152 vrf mgmt-vrf
```

To connect to a remote device using an SSH connection with a login name:

```
device# ssh -l admin 127.2.1.8
```

```
admin@127.2.1.8's password
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh client cipher

Sets the SSH client's cipher list for the SSH client.

## Syntax

`ssh client cipher string`

`no ssh client cipher`

## Parameters

*string*

The string name of the cipher. Refer to the device for the available options.

## Modes

Global configuration mode

## Usage Guidelines

Use the `no ssh client cipher` command remove the cipher list from the ssh client.

## Examples

Sets the SSH client's cipher list.

```
device# configure terminal
device(config)# ssh client cipher aes128-cbc
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh client cipher non-cbc

Sets the SSH client's cipher list to non-cbc ciphers for the SSH client.

## Syntax

`ssh client cipher non-cbc`

`no ssh client cipher non-cbc`

## Modes

Global configuration mode

## Usage Guidelines

Use the `no ssh client cipher non-cbc` command to remove the non-cbc cipher list from the ssh client.

## Examples

Sets the SSH client's cipher list to non-cbc ciphers.

```
device# configure terminal
device(config)# ssh client cipher non-cbc
device(config)# do show running-config ssh
ssh server non-cbc
ssh client non-cbc
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh client key-exchange

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server and Diffie-Hellman group 14.

## Syntax

```
ssh client key-exchange diffie-hellman-group14-sha1
```

```
no ssh client key-exchange
```

## Command Default

This command is not configured by default.

## Modes

Global configuration mode

## Usage Guidelines

You can configure the SSH client key-exchange method to DH Group 14. When the ssh client key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14. Enter **no ssh client key-exchange** to restore ssh client key-exchange to the default value.

For information on DH Group 14, refer to [RFC 3526](#).

For backward compatibility, the string "dh-group-14" is also acceptable in place of "diffie-hellman-group14-sha1"

## Examples

To set ssh client key-exchange to DH Group 14:

```
device(config)#ssh client key-exchange diffie-hellman-group14-sha1
```

To restore the ssh client key-exchange to default value:

```
device(config)# no ssh client key-exchange
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh client mac

Supports MAC configurations for the SSH client.

## Syntax

`ssh client mac string`

`no ssh client mac`

## Command Default

SSH server is enabled by default.

## Parameters

*string*

The string name of the default MAC required. Your choices are hmac-md5, hmac-sha1, hmac-sha2-256, and hmac-sha2-512. The default MACs supported in FIPS mode are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

## Modes

Global configuration mode

## Usage Guidelines

The MAC hmac-md5 is not supported in FIPS mode.

## Examples

Typical command example:

```
device# configure terminal
device(config)# ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
device(config)# do show running-config ssh client
ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
!
device(config)# do show ssh client status
SSH Client Mac: hmac-sha1,hmac-sha2-256,hmac-sha2-512
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh server cipher

Sets the SSH server's cipher list for the SSH server.

## Syntax

```
ssh server cipher string
```

```
no ssh server cipher
```

## Parameters

*string*

The string name of the cipher. Refer to the device for the available options.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no ssh server cipher** command remove the cipher list from the ssh client.

## Examples

Sets the SSH server's cipher list.

```
device# configure terminal
device(config)# ssh server cipher aes256-ctr
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# ssh server cipher non-cbc

Sets the SSH server's cipher list to non-cbc ciphers for the SSH server.

## Syntax

```
ssh server cipher non-cbc
```

```
no ssh server cipher non-cbc
```

## Modes

Global configuration mode

## Usage Guidelines

Use the **no ssh server cipher non-cbc** command remove the non-cbc cipher list from the ssh client.

## Examples

Sets the SSH server's cipher list to non-cbc ciphers.

```
device# configure terminal
device(config)# ssh server cipher non-cbc
device(config)# do show running-config ssh
ssh server non-cbc
ssh client non-cbc
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh server key

Generates or zeroizes SSH crypto keys on the device. All three keys can be active simultaneously.

## Syntax

```
ssh server key {dsa | rsa [1024 | 2048] | ecdsa 256}
```

```
no ssh server key {dsa | rsa | ecdsa}
```

## Command Default

The default values of SSH keys are:

- DSA is active
- ECDSA value is 256
- RSA value is 2048

## Parameters

**dsa**

Generates the DSA key.

**rsa [1024 | 2048]**

Generates the RSA key, in either the 1024 or 2048 bit size.

**ecdsa 256**

Generates the ECDSA key at 256 bits.

## Modes

Global configuration mode

## Usage Guidelines

The **no ssh server key** command zeroizes the SSH keys on the device.

If you generate and delete SSH crypto keys, you must restart the SSH server using the **no ssh server shutdown** command to enable the configuration.

## Examples

Typical DSA command example:

```
device(config)# ssh server key dsa
```

Typical RSA command example:

```
device(config)# ssh server key rsa 1024
```

Typical ECDSA command example:

```
device(config)# ssh server key ecdsa 256
```

Typical zeroizing example:

```
device(config)# no ssh server key dsa
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh server key-exchange

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server and Diffie-Hellman group 14.

## Syntax

```
ssh server key-exchange diffie-hellman-group14-sha1
```

```
no ssh server key-exchange
```

## Command Default

This command is not configured by default.

## Modes

Global configuration mode

## Usage Guidelines

You can configure the SSH server key-exchange method to DH Group 14. When the SSH server key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14. Enter **no ssh server key-exchange** to restore SSH server key-exchange to the default value.

For information on DH Group 14, refer to [RFC 3526](#).

For backward compatibility, the string "dh-group-14" is also acceptable in place of "diffie-hellman-group14-sha1"

## Examples

To set SSH server key-exchange to DH Group 14:

```
device(config)# ssh server key-exchange diffie-hellman-group14-sha1
```

To restore the SSH server key-exchange to default value:

```
device(config)# no ssh server key-exchange
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh server mac

Supports MAC configurations for the SSH server.

## Syntax

```
ssh server mac string
```

```
no ssh server mac
```

## Parameters

*string*

The string name of the default MAC required. Your choices are hmac-md5, hmac-sha1, hmac-sha2-256, and hmac-sha2-512. The default MACs supported in FIPS mode are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

## Modes

Global configuration mode

## Usage Guidelines

The MAC hmac-md5 is not supported in FIPS mode.

## Examples

Typical command example:

```
device# configure terminal
device(config)# ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
device(config)# do show running-config ssh server
ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
ssh server key rsa 2048
ssh server key ecdsa 256
ssh server key dsa
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh server max-sessions

Specifies the maximum number of open Secure Shell (SSH) sessions per SSH network connection.

## Syntax

```
ssh server max-sessions number  
no ssh server max-sessions
```

## Command Default

The default number of sessions is 1 unless it is changed by this command.

## Parameters

*number*  
Maximum number of sessions. Range is from 1 through 10.

## Modes

Global configuration mode

## Usage Guidelines

After executing this command, in order to use the new number of sessions, you must first shut down the SSH server, by means of the **ssh server use-vrf shutdown** command, and then restart it, by means of the **no ssh server use-vrf shutdown** command.

The maximum number of sessions specified by this command is synchronized to the standby management module (MM). However, to make the change effective on the standby MM, you must first disable service on that module by means of the **no ssh server standby enable** command, and then reenabling service by means of the **ssh server standby enable** command.

A downgrade to a previous release is blocked if this command has been executed in the running configuration.

Use the **no ssh server max-sessions** command to revert to the default of 1 session. You must also stop and restart service as in the Usage Guidelines above.

## Examples

To change the maximum number of supported SSH sessions from the default to 7, and confirm the configuration:

```
device# configure terminal  
device(config)# ssh server max-sessions 7  
device(config)# do show running-config ssh server  
ssh server max-sessions 7  
ssh server key rsa 2048  
ssh server key ecdsa 256  
ssh server key dsa
```

To revert to the default number of sessions (1):

```
device(config)# no ssh server max-sessions
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh server rekey-interval

Configures the Secure Shell (SSH) server rekey-interval.

## Syntax

`ssh server rekey-interval interval`

`no ssh server rekey-interval`

## Parameters

*interval*

The value for the rekey interval. Range is from 900 to 3600 seconds.

## Modes

Global configuration mode

## Usage Guidelines

Use the `no ssh server rekey-interval` command to remove the rekey-interval.

## History

Release version	Command history
16r.1.00	This command was introduced.



# ssh server shutdown

Disables SSH service.

## Syntax

```
ssh server [ use-vrf vrf-name ] shutdown
```

```
no ssh server [ use-vrf vrf-name ] shutdown
```

## Parameters

**use-vrf** *vrf-name*

Specifies a user-defined VRF, or built-in VRFs such as mgmt-vrf or default-vrf.

## Modes

Global configuration mode

## Usage Guidelines

Enter **no ssh server shutdown** to enable SSH service.

The use of the **use-vrf** keyword brings down the server only for the specified VRF. The user can shut down any server in any VRF, including the management and default VRF.

When this command is executed and a VRF is not specified by means of the **use-vrf** keyword, the server is brought down only in the management VRF ("mgmt-vrf") (the default VRF for this command).

## Examples

To shut down SSH service on the management VRF:

```
device(config)# ssh server shutdown
```

To shut down SSH service for a user-defined VRF:

```
device(config)# ssh server use-vrf myvrf shutdown
```

To enable SSH service on the management VRF:

```
device(config)# no ssh server shutdown
```

To enable SSH service:

```
device(config)# no ssh server shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssh server standby enable

Enables the SSH services on the standby MM.

## Syntax

`ssh server standby enable`

`no ssh server standby enable`

## Command Default

The SSH services are disabled on the standby MM.

## Modes

Global configuration mode

## Usage Guidelines

The `no ssh server standby enable` command disables the SSH services on the standby MM.

## Examples

Typical command output:

```
device(config)# no ssh server standby enable
device(config)# do show running-config | include standby
% No entries found.
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ssm-enable

Enables or disables the SSM mode for PIM.

## Syntax

```
ssm-enable range IP prefix list name
```

```
no ssm-enable range IP prefix list name
```

## Parameters

### range

Specifies the range of the SSM map.

*IP prefix list name*

Specifies the name of the IP prefix list.

## Modes

Router PIM configuration mode

## Usage Guidelines

PIM Source Specific Multicast (SSM) is a subset of the PIM SM protocol. In the PIM SSM mode, the shortest path tree (SPT) is created at the source. The SP is created between the receiver and source, but the SPT is built without the help of the RP. The router closest to the interested receiver host is notified of the unicast IP address of the source for the multicast traffic. PIM SSM goes directly to the source-based distribution tree without the need of the RP connection. PIM SSM is different from PIM SM because it forms its own SP tree, without forming a shared tree.

## Examples

The following example enables SSM and applies the default SSM range - 232.0.0.0/8.

```
device(config)# router pim
device(config-pim-router)# ssm-enable
```

The following example enables SSM and configures an SSM map at the global level.

```
device(config)# ip igmp ssm-map enable
device(config)# ip igmp ssm-map ssm-map-230-to-232 203.0.0.10
device(config)# ip igmp ssm-map ssm-map-233-to-234 204.0.0.10
```

The following example configures the SSM range at the router PIM configuration level.

```
device(config)# router pim
device(config-pim-router)# ssm-enable range PL_ssm_range -230-to-234
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# start-shell

Accesses the MMVM Linux shell from the CLI.

## Syntax

**start-shell**

## Command Default

Not applicable.

## Modes

Privileged EXEC

## Usage Guidelines

This command is only visible in the CLI when you are configured as a user with the admin role.

Inside the MMVM Linux shell, you will have root level privilege and can run all supported Linux commands.

## Examples

The following example accessed the MMVM Linux shell from the CLI.

```
device# start-shell
Entering Linux shell for the user: admUser

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[admUser@SLX] #
```

The following example exits the shell and returns to the CLI.

```
[admUser@SLX]# exit
exit
Exited from Linux shell
device#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# static-network

Configures a static BGP4 network, creating a stable network in the core.

## Syntax

**static-network** *network/mask* [ **distance** *num* ]

**no static-network** *network/mask* [ **distance** *num* ]

## Command Default

This option is not enabled.

## Parameters

*network/mask*

Network and mask in CIDR notation.

**distance** *num*

Specifies an administrative distance value for this network. Range is from 1 through 255. The default is 200.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

## Usage Guidelines

While a route configured with this command will never flap unless it is deleted manually, a static BGP4 network will not interrupt the normal BGP4 decision process on other learned routes that are installed in the Routing Table Manager (RTM).

Consequently, when there is a route that can be resolved, it will be installed into the RTM.

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

## Examples

The following example configures a static network and sets an administrative distance of 300.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# static-network 10.11.12.0/32 distance 300
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# statistics

Enables statistics on the tunnel interface.

## Syntax

**statistics**

**no statistics**

## Command Default

Statistics is disabled on a tunnel interface.

## Modes

Interface tunnel configuration mode

## Usage Guidelines

Use the **no** form of this command to disable statistics on the tunnel interface.

Note that traffic loss might occur when you enable or disable statistics on a tunnel interface.

## Examples

This example enables statistics on the tunnel interface.

```
device# configure terminal
device (config)# interface tunnel 5
device(config-intf-tunnel-5)# statistics
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# statistics (bridge domain)

Enables ingress and egress statistics on a bridge domain.

## Syntax

**statistics**

**no statistics**

## Parameters

None

## Command Default

Statistics are disabled.

## Modes

Bridge-domain configuration mode.

## Usage Guidelines

The **no** form of the command disables statistics on the bridge domain.

## Examples

The following example shows how to enable ingress and egress statistics on bridge domain 2.

```
device# config terminal
device(config)# bridge-domain 2
device(config-bridge-domain-2)# statistics
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# statistics (VLAN)

Enables statistics on a VLAN.

## Syntax

**statistics**

**no statistics**

## Command Default

Statistics are disabled.

## Parameters

None

## Modes

VLAN configuration mode

## Usage Guidelines

The **no** form of the command disables statistics on a VLAN.

## Examples

The following example shows how to enable statistics on VLAN 10.

```
device# config terminal
device(config)# vlan 10
device(config-Vlan-10)# statistics
```

## History

Release version	Command history
16r.1.01	This command was introduced.

# storm-control ingress

Limits ingress traffic on a specified interface.

## Syntax

```
storm-control ingress { broadcast | unknown-unicast | multicast } { limit-bps | limit-percent } rate [ { monitor | shutdown } ]
no storm-control ingress { broadcast | unknown-unicast | multicast } { limit-bps | limit-percent } rate [ { monitor | shutdown } ]
```

## Parameters

### broadcast

Specifies that the command will operate on broadcast traffic only.

### unknown-unicast

Specifies that the command will operate on unknown-unicast traffic only.

### multicast

Specifies that the command will operate on multicast traffic only.

### limit-bps

Specifies that the value given to the *rate* parameter is in bits per second. If the traffic on the interface reaches this rate, no more traffic (for the traffic type specified) is allowed on the interface.

### limit-percent

Specifies that the value given to the *rate* parameter is in percentage of capacity of the interface. If the traffic on the interface reaches this percentage of capacity, no more traffic (for the traffic type specified) is allowed on the interface.

### rate

Specifies the amount of traffic allowed, either in bits per second or a percentage of the capacity of the interface, depending on which parameter was chosen with the rate.

- Range if you are specifying rate in bps: 0 to 10000000000. Because each application-specific integrated circuit (ASIC) may support different bit granularity, bit rates are rounded up to the next achievable rate.
- Range if you are specifying rate in percent of interface capacity: 0 to 100.

### monitor

Specifies that, if a rate limit is reached within a five-second sampling period, a log message gets sent. A log message is generated upon the first occurrence of such an event. Subsequent log messages are generated only at the end of one complete sample interval in which no rate limits are reached.

### shutdown

Specifies that, if a rate limit is exceeded within a five-second sampling period, the interface will be shut down. You must manually re-enable the interface after a shutdown.

## Modes

Interface configuration mode

## Usage Guidelines

This command limits the amount of broadcast, unknown unicast, and multicast (BUM) ingress traffic on a specified interface. The *shutdown* parameter monitors the status of the configured rate limit every five seconds, and if the maximum defined rate is exceeded the corresponding interface is shut down until you re-enable it using the **no shut** command.

If you want to modify an active BUM storm control configuration, you must first disable it, then issue the **storm-control ingress** command again with the new parameters.

Enter **no storm-control ingress** to disable BUM storm control for a particular traffic type on an interface.

## Examples

To configure storm control on an Ethernet interface, with a rate limited to 1000000 bps:

```
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# storm-control ingress broadcast 1000000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# subnet

Specifies the local IP address with the subnet mask of the routing device.

## Syntax

```
subnet { subnet_addr }
no subnet { subnet_addr }
```

## Command Default

The command is disabled, by default.

## Parameters

*subnet\_addr*  
Specifies the subnet mask of the IP address.

## Modes

MPLS CSPF-group configuration mode.

## Usage Guidelines

When the command is configured, every link in the subnet is penalized.

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

## Examples

The following example configures subnet *10.1.2.0* with a mask length of *24*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# cspf-group group3
device(config-router-mpls-cspf-group-group3)# subnet 10.1.2.0/24
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# summary-address (IS-IS)

Configures route summarization to aggregate Intermediate System-to-Intermediate System (IS-IS) route information.

## Syntax

**summary-address** *ip-address subnet-mask level-1* [ *level-2* ]

**summary-address** *ip-address subnet-mask level-2* [ *level-1* ]

**no summary-address** *ip-address subnet-mask level-1* [ *level-2* ]

**no summary-address** *ip-address subnet-mask level-2* [ *level-1* ]

## Command Default

Disabled.

## Parameters

*ip-address*

Specifies an IP address.

*subnet-mask*

Specifies a subnet mask.

**level-1**

Specifies that only routes redistributed into Level 1 are summarized with the configured address and mask value.

**level-2**

Specifies that only routes redistributed into Level 2 are summarized with the configured address and mask value.

## Modes

IS-IS address-family IPv4 unicast configuration mode

## Usage Guidelines

Route Summarization using this command is applicable only for redistributed routes.

The **no** form of the command disables route summarization.

## Examples

The following example configures a summary address of 10.1.0.0 with a mask of 255.255.0.0 for Level 1 redistributed routes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-address 10.1.0.0 255.255.0.0 level-1
```

The following example configures a summary address of 10.1.0.0 with a mask of 255.255.0.0 for Level 2 redistributed routes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-address 10.1.0.0 255.255.0.0 level-2
```

The following example configures a summary address of 10.1.0.0 with a mask of 255.255.0.0 for Level 1 and Level 2 redistributed routes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-address 10.1.0.0 255.255.0.0 level-1 level-2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# summary-address (OSPFv2)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

## Syntax

```
summary-address A.B.C.D E.F.G.H  
no summary-address
```

## Command Default

Summary addresses are not configured.

## Parameters

*A.B.C.D E.F.G.H*  
IP address and mask for the summary route representing all the redistributed routes in dotted decimal format.

## Modes

OSPF router configuration mode  
OSPF VRF router configuration mode

## Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges. This parameter affects only imported, type 5 external routes.

The no form of the command disables route summarization.

## Examples

The following example configures a summary address of 10.1.0.0 with a mask of 10.255.0.0:

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# summary-address 10.1.0.0 10.255.0.0
```

### NOTE

The command in this example configures summary address 10.1.0.0, which includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. For all of these networks, only the address 10.1.0.0 is advertised in external LSAs.

## History

Release version	Command history
16r.1.00	This command was introduced.



# summary-address (OSPFv3)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

## Syntax

```
summary-address IPv6-addr/mask  
no summary-address
```

## Command Default

Summary addresses are not configured.

## Parameters

*A:B:C:D/LEN*

IPv6 address and mask for the summary route representing all the redistributed routes in dotted decimal format.

## Modes

OSPFv3 router configuration mode  
OSPFv3 VRF router configuration mode

## Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified IPv6 address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow condition, all the imported routes are summarized according to the configured address ranges.

## Examples

The following example configures a summary address of 2001:db8::/24 for routes redistributed into OSPFv3.

```
device# configure terminal  
device(config)# ipv6 router ospf  
device(config-ipv6-router-ospf-vrf-default-vrf)# 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.

## History

Release version	Command history
16r.1.00	This command was introduced.

# summary-prefix

Configures summary prefixes to aggregate IPv6 Intermediate System-to-Intermediate System (IS-IS) route information.

## Syntax

```
summary-prefix ipv6-prefix prefix-length { level-1 | level-2 }
```

```
no summary-prefix ipv6-prefix prefix-length { level-1 | level-2 }
```

## Command Default

Disabled.

## Parameters

*ipv6-prefix prefix-length*

Specifies the aggregate address. You must specify the *ipv6-prefix* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. You must specify the *prefix-length* parameter as a decimal value. A slash mark (/) must follow the *ipv6-prefix* parameter and precede the *prefix-length* parameter.

**level-1**

Specifies that only routes redistributed into Level 1 are summarized

**level-2**

Specifies that only routes redistributed into Level 2 are summarized.

## Modes

IS-IS address-family IPv6 unicast configuration mode

## Usage Guidelines

Route Summarization using this command is applicable only for redistributed routes.

The **no** form of the command disables route summarization.

## Examples

The following example configures a summary prefix of 2001:db8::/32 to be advertised to Level 1 redistributed routes only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-prefix 2001:db8::/32 level-1
```

The following example configures a summary prefix of 2001:db8::/32 to be advertised to Level 2 redistributed routes only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-prefix 2001:db8::/32 level-2
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# switch-attributes

Configures the chassis or host name for the device.

## Syntax

```
switch-attributes { chassis-name chassis-name } | { host-name host-name }  
switch-attributes { chassis-name | host-name }
```

## Command Default

The default chassis name is SLX9850-# where # is the number of slots in the chassis.

The default host name is SLX.

## Parameters

**chassis-name** *chassis-name*

Specifies the chassis name. A chassis name can be from 1 through 30 characters long, must begin with a letter, and can contain letters, numbers, and underscore characters.

**host-name** *host-name*

Specifies the host name and changes the CLI prompt. A host name can be from 1 through 30 characters long. It must begin with a letter, and can contain letters, numbers, and underscore characters.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no** form of the command to reset the default settings.

Extreme Networks recommends that you customize the chassis name for each device. Some system logs identify the device by its chassis name; if you assign a meaningful chassis name, logs are more useful.

## Examples

The following example configures the chassis and host names.

```
device# configure terminal  
device(config)# switch-attributes chassis-name SLX-market1  
device(config)# switch-attributes host-name SLX-mrkt  
SLX-mrkt(config)#
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# switchport port-security

Enables port security on an interface port.

## Syntax

**switchport port-security**

**no switchport port-security**

## Command Default

Port security is not enabled.

## Modes

Interface configuration mode

## Usage Guidelines

Port mode change is not allowed when port security is enabled on the interface.

The **no switchport port-security** command disables port security on the interface.

## Examples

The following example enables port MAC security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# switchport port-security mac-address

Configures the MAC address option for port security on an interface port.

## Syntax

```
switchport port-security mac-address address vlan vlan_id
```

## Command Default

MAC address is not configured for port security.

## Parameters

**mac-address** *address*

Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

**vlan** *vlan\_id*

Specifies a VLAN.

## Modes

Interface configuration mode

## Usage Guidelines

Static MAC addresses cannot be configured on a secure port. They must be configured as secure MAC addresses on the secure port.

When static MAC address is configured on an access secure port, the MACs qualify for access VLANs, but on trunk port, VLAN must be specified.

The **no switchport port-security mac-address** command removes the specified MAC address.

## Examples

The following example configures static MAC address for port security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security mac-address 0000.00eb.2d14 vlan 2
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# switchport port-security max

Configures the maximum number of MAC addresses used for port MAC security on an interface port.

## Syntax

```
switchport port-security max value
no switchport port-security max
```

## Parameters

*value*

The maximum number of secure MAC addresses. Range is from 1 through 8192.

## Command Default

The default value is 8192 MAC addresses.

## Modes

Interface configuration mode

## Usage Guidelines

The maximum MAC address limit for sticky MAC address and static MAC address depends on the device limit. For dynamically learned MAC addresses, the maximum limit is 8192 per port.

The **no switchport port-security max** command restores the default value of maximum number of MAC addresses.

## Examples

The following example configures the maximum number of MAC addresses used for port MAC security on an interface port as 10:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security max 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# switchport port-security shutdown-time

Configures the auto recovery time for ports that shuts down following a port security violation on an interface.

## Syntax

```
switchport port-security shutdown-time time
```

## Command Default

Auto recovery of ports is not enabled.

## Parameters

*time*

The amount of time in minutes, the port waits before it recovers from forced port shutdown. Range is from 1 through 15.

## Modes

Interface configuration mode

## Usage Guidelines

The shutdown and no-shutdown processes initiated as part of the port violation action is independent of the shutdown process explicitly initiated by an administrator on the same port on which port MAC security is enabled.

If a port security-based change occurs when a port is shut down, the shutdown timer is not triggered. Consequently, the user must restore the full functionality of the port.

When port security violation causes a port to be shut down and the user manually changes the shutdown time, the shutdown timer is reset and the timer starts with the new shutdown time.

The **no switchport port-security shutdown-time** command disables the auto recovery functionality.

## Examples

The following example configures the auto recovery time as 4 minutes for ports that shuts down following a port security violation on an interface.

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security shutdown-time 4
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# switchport port-security sticky

Enables sticky MAC learning on the port to convert the dynamically learned MAC addresses to sticky secure MAC addresses.

## Syntax

```
switchport port-security sticky [ mac-address address vlan vlan_id ]
```

```
no switchport port-security sticky [ mac-address address vlan vlan_id ]
```

## Command Default

Sticky MAC learning on the port is not enabled.

## Parameters

**mac-address** *address*

Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

**vlan** *vlan\_id*

Specifies a VLAN.

## Modes

Interface configuration mode

## Usage Guidelines

When sticky MAC learning is enabled on a secured port, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All the subsequent sets of dynamically learned MAC addresses will also be converted to sticky secure MAC addresses.

The **no switchport port-security sticky** disables sticky MAC learning on a secure port, and all the sticky MAC addresses will be converted back to dynamically learned MAC addresses.

Sticky MAC addresses persist even if the port goes down or if the device reboots.

## Examples

The following example enables sticky MAC learning on the port and configures port security with sticky MAC address:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security sticky
device(conf-if-eth-3/2)# switchport port-security sticky mac-address 0000.0018.747C vlan 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# switchport port-security violation

Configures the violation response action for port security on an interface.

## Syntax

```
switchport port-security violation shutdown
```

## Command Default

The port shuts down if port security violation occurs.

## Parameters

**shutdown**

Puts the interface into the error-disabled state.

## Modes

Interface configuration mode

## Usage Guidelines

If a MAC address already learned on a secured port ingresses on a non-secured port or through another secured port, it is not considered security violation. In this scenario, MAC movement happens if it is a dynamically learned MAC address. If it is a static MAC address or sticky MAC address, MAC movement does not happen, but the traffic is switched (flooded or forwarded) based on the destination MAC address.

If the port shuts down after security violation, an administrator can explicitly bring up the interface or a shutdown timer can be configured using the **switchport port-security shutdown-time** command. After the configured shutdown time, the interface automatically comes up and the port security configuration remains configured on the port.

When the device reboots after port shutdown due to security violation, the ports come up in the shutdown state.

## Examples

The following example configures the violation response action as shutdown for port security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security violation shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# system-description

Sets the global system description specific to LLDP.

## Syntax

`system-description` *line*

`no system-description`

## Parameters

*line*

Specifies a description for the LLDP system. The string must be between 1 and 50 ASCII characters in length.

## Modes

Protocol LLDP configuration mode

## Usage Guidelines

Enter `no system-description` to clear the global LLDP system description.

## Examples

To set the global system description specific to LLDP on the SLX-OS platform, enter the following:

```
device(conf-lldp)# system-description SLXR
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# system-name

Sets the global system name specific to LLDP.

## Syntax

**system-name** *name*

**no system-name**

## Command Default

The host name from the device is used.

## Parameters

*name*

Specifies a system name for the LLDP. The string must be between 1 and 32 ASCII characters in length.

## Modes

Protocol LLDP configuration mode

## Usage Guidelines

Enter **no system-name** to delete the name.

## Examples

To specify a system name for the LLDP:

```
device(conf-lldp)# system-name System10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# table-map

Maps external entry attributes into the BGP routing table, ensuring that those attributes are preserved after being redistributed into OSPF.

## Syntax

**table-map** *string*

**no table-map** *string*

## Command Default

This option is disabled.

## Parameters

*string*

Specifies a route map to be whose attributes are to be preserved. Range is from 1 through 63 ASCII characters.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

Use the **no** form of the command to remove the table map.

Use this command only to set the tag values. Normally, a route map is applied on routes (and therefore the routes are updated) before it is stored in the BGP routing table. Use the **table-map** command to begin the update before the routes are stored in the IP routing table.

Configurations made by this command apply to all peers.

Route maps that contain **set** statements change values in routes when the routes are accepted by the route map. For inbound route maps (route maps that filter routes received from neighbors), the routes are changed before they enter the BGP routing table. For tag values, if you do not want the value to change until a route enters the IP routing table, you can use a table map to change the value. A table map is a route map that you have associated with the IP routing table. The device applies the **set** statements for tag values in the table map to routes before adding them to the routing table. To configure a table map, you first configure the route map, then identify it as a table map. The table map does not require separate configuration. You can have only one table map.

**NOTE**

Use table maps only for setting the tag value. Do not use table maps to set other attributes. To set other route attributes, use route maps or filters. To create a route map and identify it as a table map, enter commands such those shown in the first example below. These commands create a route map that uses an address filter. For routes that match the IP prefix list filter, the route map changes the tag value to 100 and is then considered as a table map. This route map is applied only to routes that the device places in the IP routing table. The route map is not applied to all routes. The first example below assumes that IP prefix list p11 has already been configured.

## Examples

This example illustrates the execution of the **table-map** command.

```
device# configure terminal
device(config)# route-map tag_ip permit 1
device(config-route-map/tag_ip/permit/1)# match ip address prefix-list p11
device(config-route-map/tag_ip/permit/1)# set tag 100
device(config-route-map/tag_ip/permit/1)# exit
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# table-map tag_ip
```

This example removes the table map for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no table-map tag_ip
```

This example removes the table map for VRF "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# no table-map tag_ip
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# tacacs-server

Configures a Terminal Access Controller Access-Control System plus (TACACS+) server.

## Syntax

```
tacacs-server {host hostname | source-ip [ chassis-ip | mm-ip ]} [ port portnum ] [ protocol { chap | pap } ] [ key shared_secret ] [ encryption-level value_level ] [ timeout secs ] [ retries num ] [ use-vrf vrf-name ]
```

```
no tacacs-server { host hostname | source-ip [ chassis-ip | mm-ip ]} [ use-vrf vrf-name ]
```

## Command Default

Refer to the Parameters section for specific defaults.

## Parameters

### host *hostname*

Specifies the IP address or domain name of the TACACS+ server. IPv4 and IPv6 addresses are supported.

### source-ip [*chassis-ip* | *mm-ip*]

Specifies the chassis IP address or MM IP address as the source IP address for TACACS+ authentication and accounting.

### port *portnum*

Specifies the authentication port. Valid values range from 0 through 65535. The default is 49.

### protocol { *chap* | *pap* }

Specifies the authentication protocol. Options include CHAP and PAP. The default is CHAP.

### key *shared\_secret*

Specifies the text string that is used as the shared secret between the device and the TACACS+ server to make the message exchange secure. The key must be between 8 and 40 characters in length. The default key is **sharedsecret**. The exclamation mark (!) is supported both in RADIUS and TACACS+ servers, and you can specify the password in either double quotes or the escape character (\), for example "**secret!key**" or **secret\!key**.

### encryption-level *value\_level*

Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The valid values are 0 and 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 7.

### timeout *secs*

Specifies the time to wait for the TACACS+ server to respond. The default is 5 seconds.

### retries *num*

Specifies the number of attempts allowed to connect to a TACACS+ server. The default is 5 attempts.

### use-vrf *vrf-name*

Specifies a VRF through which to communicate with the TACACS+ server. See the Usage Guidelines.

## Modes

Global configuration mode

## Usage Guidelines

If a TACACS+ server with the specified IP address or host name does not exist, it is added to the server list. If the TACACS+ server already exists, this command modifies the configuration. The **key** parameter does not support an empty string.

Executing the **no** form of the **tacacs-server** command attributes resets the specified attributes to their default values.

### NOTE

Before downgrading to a software version that does not support the **encryption-level** keyword, set the value of this keyword to **0**. Otherwise, the firmware download will throw an error that requests this value be set to **0**.

Before downgrading to a version that doesn't support **tacacs-server source-ip**, you must remove the source-ip configuration using **no tacacs-server source-ip**. Otherwise, the firmware download process throws an error requesting to reset the cipher.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

## Examples

To configure an IPv4 TACACS+ server:

```
device(config)# tacacs-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# protocol chap retries 100
device(config-host-10.24.65.6/mgmt-vrf)# tacacs-server source-ip chassis-ip
device(config-host-10.24.65.6/mgmt-vrf)#
```

To modify an existing TACACS+ server configuration:

```
device(config)# tacacs-server host 10.24.65.6
device(config-tacacs-server-10.24.65.6/mgmt-vrf)# key "changedsec"
```

To delete a TACACS+ server:

```
device(config)# no tacacs-server host 10.24.65.6
device(config)# exit
device# show running-config tacacs-server host 10.xx.xx.xxx
tacacs-server host 10.xx.xx.xxx use-vrf mgmt-vrf
  key "KfDRG/hc15qxsRjUIZrJw==\n" encryption-level 7
!
```

To configure an IPv6 TACACS+ server:

```
device(config)# tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)# protocol chap key "mysecret"
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)# tacacs-server source-ip
chassis-ip
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)#
```

## History

Release version	Command history
16.r.1.00	This command was introduced.

# telnet

Establishes a Telnet session to a remote networking device.

## Syntax

```
telnet IP_address [ port-number port_number ] [ vrf name ]
```

```
telnet hostname } [ port-number port_number ] [ interface { ethernet slot/port } | management | { ve number } ] [ vrf name ]
```

## Command Default

The default port is 23.

## Parameters

*IP\_address*

The server IP address in either IPv4 or IPv6 format.

**port-number** *port*

Specifies the port number in the remote device to connect to. Range is from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

**vrf** *vrf-name*

Specifies a VRF instance. See the Usage Guidelines.

*hostname*

Specifies the host name which is a string between 1 and 63 ASCII characters in length.

**port-number** *port*

Specifies the port number in the remote device to connect to. Range is from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

**interface**

Specifies an interface.

**ethernet** *slot/port*

Specified the Ethernet interface slot and port number.

**management**

Specifies a management interface.

**ve** *VE-id*

Specifies the VE interface number.

## Modes

Privileged EXEC mode

## Usage Guidelines

You can override the default port. However, the device must be listening on this port for the connection to succeed.

The following features are not supported:

- Display Telnet sessions
- Ability to terminate hung Telnet sessions

## Examples

The following example establishes a Telnet connection to a remote device.

```
device# telnet 10.20.51.68 vrf mgmt-vrf
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# telnet server

Configures the Telnet server on the device.

## Syntax

```
telnet server standby enable
```

```
telnet server [ use-vrf name ] shutdown
```

```
no telnet server {standby | { [use-vrf name ] shutdown}}
```

## Command Default

The Telnet service is enabled by default.

Telnet service on the standby MM is disabled.

## Parameters

### standby enable

Enables the Telnet server on the standby management module (MM).

### use-vrf *name*

Specifies a user-defined VRF.

### shutdown

Disables the Telnet server.

## Modes

Global configuration mode

## Usage Guidelines

Use the **no** form of the command to disable the standby MM Telnet service, or re-enable the Telnet service on the device. If you include the VRF name, the Telnet server for the VRF is re-enabled.

Shutting down the Telnet service forcibly disconnects all Telnet sessions running on a device.

When you use the **telnet server shutdown** command without a user-defined VRF, the service is shut down on mgmt-vrf only.

Telnet services are associated and started on mgmt-vrf and default-vrf.

Telnet server can be enabled on a maximum number of six VRFs.

## Examples

The following example shuts down the Telnet server on the device.

```
device# configure terminal
device(config)# telnet server shutdown
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# terminal

Sets terminal parameters for the current session.

## Syntax

**terminal length** *lines*

**terminal monitor**

**terminal no length**

**terminal timeout** *seconds*

**no terminal** { **monitor** | **timeout** }

## Command Default

The terminal length is 24 lines.

The terminal timeout is 600 seconds (10 minutes).

## Parameters

**length** *number\_of\_lines*

Specifies the number of lines to be displayed. Valid values range from 1 through 512. Specify 0 for infinite length.

**monitor**

Enables terminal monitoring.

**timeout** *seconds*

Specifies the timeout value in minutes. Enter an integer from 1 to 8192. Specify 0 to disable the timeout.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use the **no** form of the command to reset the default timeout or disable monitoring.

Use the **terminal no length** command to reset the default number of displayed lines.

The **timeout** overrides the timeout configuration set by the **line vty exec-timeout** command, but only for the duration of the current session. When the current session ends, the configured values apply for any subsequent sessions.

## Examples

The following example sets the display length to 30 lines.

```
device# terminal length 30
```

The following example sets timeout length to 3600 seconds (60 minutes).

```
device# terminal timeout 3600
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# threshold-monitor cpu

Configures monitoring of CPU usage of the system and alerts the user when configured thresholds are exceeded.

## Syntax

```
threshold-monitor cpu { [ actions [ none | raslog [ { limit limit_when_reached | poll polling_interval | retry
    number_of_retries ] ] ] }
```

```
no threshold-monitor cpu
```

## Parameters

### actions

Specifies the action to be taken when a threshold is exceeded.

### none

No action is taken.

### raslog

Specifies RASLog messaging.

### limit

Specifies the baseline CPU usage limit as a percentage of available resources.

#### *limit\_when\_reached*

When the limit set by this parameter is exceeded, a RASLog WARNING message is sent. When the usage returns below the limit, a RASLog INFO message is sent. Valid values range from 0 through 80 percent. The default is 70 percent.

### poll

Specifies the polling interval in seconds.

#### *polling\_interval*

The range is from 0 through 3600. The default is 120

### retry

Specifies the number of polling retries before desired action is taken.

#### *number\_of\_retries*

Range is from 1 through 100. The default is 3.

## Modes

Global configuration mode

## Usage Guidelines

This command sends a RASLog WARNING message when configured thresholds are exceeded.

threshold-monitor cpu

## Examples

```
device(config)# threshold-monitor cpu actions rasloglimit 50 poll10
```

# threshold-monitor memory

Configures monitoring of the memory usage of the system and alerts the user when configured thresholds are exceeded.

## Syntax

```
threshold-monitor memory { [ actions [ none | raslog { high-limit percent | limit percent | low-limit percent | poll
polling_interval | retry number_of_retries } | high-limit percent | limit percent | low-limit percent | poll polling_interval | retry
number_of_retries ] ] }
```

```
no threshold-monitor memory
```

## Parameters

### actions

Specifies the action to be taken when a threshold is exceeded.

#### *none*

No action is taken. This is the default.

### raslog

Specifies RASLog messaging.

### high-limit

Specifies an upper limit for memory usage as a percentage of available memory.

#### *percent*

This value must be greater than the value set by **limit** . When memory usage exceeds this limit, a RASLog CRITICAL message is sent. Values range from 0 through 80 percent. The default is 70 percent.

### limit

Specifies the baseline memory usage limit as a percentage of available resources.

#### *percent*

When this value is exceeded, a RASLog WARNING message is sent. When the usage returns below the value set by **limit** , a RASLog INFO message is sent. Values range from 0 through 80 percent. The default is 60 percent.

### low-limit

Specifies a lower limit for memory usage as percentage of available memory.

#### *percent*

This value must be smaller than the value set by **limit** . When memory usage exceeds or falls below this limit, a RASLog INFO message is sent. The default is 40 percent.

### poll

Specifies the polling interval in seconds.

#### *polling\_interval*

The range is from 0 through 3600. The default is 120

### retry

Specifies the number of polling retries before desired action is taken.

threshold-monitor memory

*number\_of\_retries*

Range is from 1 through 100. The default is 3.

## Modes

Global configuration mode

## Examples

```
device(config)# threshold-monitor memory actions none high-limit 80 low-limit 50 limit 70 retry 2 poll  
30
```

# threshold-monitor sfp

Configures monitoring of SFP parameters.

## Syntax

```
threshold-monitor sfp { [ apply policy_name | pause | policy policy_name ] type SFP_type area parameters alert [ above
  [ highthresh-action [ [ all | lowthresh-action ] | email | none | raslog ] | lowthresh-action [ all | email none | raslog ] | below
  [ highthresh-action [ all | email | none raslog ] | lowthresh-action [ all | email | none | raslog ] ] | threshold [ buffer | high-
  threshold | low-threshold | timebase [ day | hour | minute | none ] ] ] }
```

```
no threshold-monitor sfp
```

## Command Default

By default, SFP is not monitored.

## Parameters

**apply** *policy\_name*

Applies a custom policy that has been created by the **policy** operand.

**pause**

Pause monitoring.

**policy**

Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.

*policy\_name*

Name of a custom policy configuration that can be saved and applied by means of the **apply** operand.

**type**

Specifies the SFP type. Possible completions are as follows:

**1GLR**

— SFP Type 1GLR

**1GSR**

— SFP Type 1GSR

**10GLR**

— SFP Type 10GLR

**10GSR**

— SFP Type 10GSR

**10GUSR**

— SFP Type 10GUSR

**100GSR**

— SFP Type 100GSR

**QSFP**

— SFP type QSFP

**area**

Specifies one of the following SFP parameters to be monitored. See Defaults, below.

**Current**

Measures the current supplied to the SFP transceiver.

**RXP**

Measures the incoming laser power, in microWatts ( $\mu$ W).

**TXP**

Measures the outgoing laser power, in  $\mu$ W).

**Temperature**

Measures the temperature of the SFP, in degrees Celsius.

**Voltage**

Measures the voltage supplied to the SFP.

**alert**

Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

**above**

Enables setting a value for **highthresh-action**, which specifies the action to be taken when a high threshold is exceeded.

**below**

Enables setting a value for **highthresh-action** and **lowthresh-action**, which specifies the action to be taken when a low threshold is exceeded.

**all**

Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of **highthresh-action** only.

**all**

Specifies that email and RASLog messaging are used.

**email**

Specifies that an email message is sent.

**none**

Specifies that no alert is sent.

**raslog**

Specifies RASLog messaging.

**limit**

Specifies the percent of threshold usage, from 0 through 80. The default is 75.

**poll**

Specifies the polling interval in seconds, from 0 through 3600. The default is 120.

**retry**

Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.

**threshold**

Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.

**buffer**

An integer value.

**high-threshold**

An integer value.

**low-threshold**

An integer value.

**timebase**

Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.

**day**

Calculates the difference between a current data value and that value a day ago.

**hour**

Calculates the difference between a current data value and that value an hour ago.

**minute**

Calculates the difference between a current data value and that value a minute ago.

**none**

Compares a data value to a threshold boundary level.

## Modes

Global configuration mode

## Examples

A typical command might look like this:

```
device(config)# threshold-monitor sfp custom type QSFP area rxp threshold high-threshold 2000 low-threshold 1000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# tie-breaking

The user can optionally configure the device to choose the path that has either the highest available bandwidth or the lowest available bandwidth.

## Syntax

```
tie-breaking { [ least-fill | most-fill | random ] }
no tie-breaking { [ least-fill | most-fill | random ] }
```

## Command Default

The default is the tie-breaking random mode.

## Parameters

### least-fill

Causes CSPF to choose the path with the highest available bandwidth (that is, the path with the least utilized links).

### most-fill

Causes CSPF to choose the path with the lowest available bandwidth (that is, the path with the most utilized links).

### random

Causes CSPF to choose the path randomly from the equal-cost paths.

## Modes

MPLS LSP configuration mode (`config-router-mpls-lsp-lsp_name`).

## Usage Guidelines

The **no** form of the command removes the tie-breaking configuration and reverts to the default mode.

## Examples

in the following example, the configuration causes the CSPF to select the path with the highest available bandwidth when choosing among equal cost paths calculated for LSP *tunnel1*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# tie-breaking least-fill
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# timers (BGP)

Adjusts the interval at which BGP KEEPALIVE and HOLDDTIME messages are sent.

## Syntax

```
timers { keep-alive keepalive_interval hold-time holdtime_interval }
```

```
no timers
```

## Command Default

The keepalive timer is 60 seconds. The hold timer is 180 seconds.

## Parameters

**keep-alive** *keepalive\_interval*

Frequency in seconds with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

**hold-time** *holdtime\_interval*

Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

## Modes

BGP configuration mode

## Usage Guidelines

Use the **no timers** command to clear the timers.

The KEEPALIVE and HOLDDTIME message interval is overwritten when the **fast-external-failover** command takes effect on a down link to a peer.

You must enter a value for **keep-alive** before you can enter a value for **hold-time**. Both values must be entered. If you only want to adjust the value of one parameter, enter the default value of the parameter that you do not want to adjust.

## Examples

The following example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# timers keep-alive 120 hold-time 360
```

The following example sets the keepalive timer for a device to 0 seconds and the hold-timer to 0 seconds so that the device waits indefinitely for messages from a neighbor without tearing down the session.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# timers keep-alive 0 hold-time 0
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# timers (OSPFv2)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) throttle timers.

## Syntax

```
timers { lsa-group-pacing interval | throttle spf start hold max }
```

## Command Default

See the parameters section for specific defaults.

## Parameters

### lsa-group-pacing *interval*

Specifies the interval at which OSPF LSAs are collected into a group and refreshed, check-summed, or aged by the OSPF process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

### throttle spf

Specifies start, hold and maximum wait intervals for throttling SPF calculations for performance. The values you enter are in milliseconds.

#### *start*

Initial SPF calculation delay. Valid values range from 0 to 60000 milliseconds. The default is 0.

#### *hold*

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

#### *max*

Maximum wait time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

## Modes

OSPF router configuration mode

OSPF VRF router configuration mode

## Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

Enter the **no timers lsa-group-pacing** to restore the pacing interval to its default value.

Enter **no timers throttle spf** to set the SPF timers back to their defaults.

## Examples

The following example sets the LSA group pacing interval to 30 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

The following example sets the SPF delay to 10000 milliseconds, the hold time to 15000 milliseconds, and the maximum wait time to 30000 milliseconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# timers throttle spf 10000 15000 30000
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# timers (OSPFv3)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) timers.

## Syntax

```
timers { lsa-group-pacing interval | spf start hold }
```

## Command Default

Enabled.

## Parameters

### lsa-group-pacing *interval*

Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check-summed, or aged by the OSPFv3 process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

### spf

Specifies start and hold intervals for SPF calculations for performance. The values you enter are in milliseconds.

#### *start*

Initial SPF calculation delay. Valid values range from 0 to 65535 seconds.

#### *hold*

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 65535 seconds.

## Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

## Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

The **no timers lsa-group-pacing** command restores the pacing interval to its default value.

The **no timers spf** command sets the SPF timers back to their defaults.

## Examples

The following example sets the LSA group pacing interval to 30 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

The following example sets the SPF delay time to 10 and the hold time to 20.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# timers spf 10 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# topology-group

Configures the topology group.

## Syntax

```
topology-group group-id
```

```
no topology-group group-id
```

## Command Default

A topology group is not configured.

## Parameters

*group-id*

Specifies the topology group ID. The ID ranges from 1 through 256.

## Modes

Global configuration mode

## Usage Guidelines

Each topology group contains a master VLAN and can contain one or more member VLANs and VLAN groups. You must configure the master VLAN and member VLANs or member VLAN groups before you configure the topology group.

You can configure up to 30 topology groups. Each group can control up to 4096 VLANs. A VLAN cannot be controlled by more than one topology group. The topology group must contain a master VLAN and can also contain individual member VLANs, VLAN groups, or a combination of individual member VLANs and VLAN groups.

The **no** form of the command removes the topology group.

## Examples

The following example configures the topology group with ID 2 and adds master VLAN and member VLANs.

```
device# configure terminal
device(config)# topology-group 2
device(config-topo-group-2)# master-vlan 2
device(config-topo-group-2)# member-vlan 3
device(config-topo-group-2)# member-vlan 4
device(config-topo-group-2)# member-vlan 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# traceroute

Traces the network path of packets as they are forwarded to a destination address.

## Syntax

```
traceroute { IPv4_address | host-name | ipv6 [ dest-ipv6-addr | host-name ] } [ interface ] [ maxttl value ] [ minttl value ] [ src-addr src-addr ] [ timeout seconds ] [ vrf vrf-name ]
```

## Parameters

*IPv4\_address*

Specifies the IPv4 address of the destination device.

*host-name*

Specifies the hostname of the destination device.

**ipv6** *dest-ipv6-addr*

Specifies the IPv6 address of the destination device.

**interface**

Selects the output interface.

**maxttl** *value*

Maximum Time To Live value in a number of hops.

**minttl** *value*

Minimum Time To Live value in a number of hops.

**src-addr** *address*

Specifies the IPv4 or IPv6 address of the source device.

**timeout** *seconds*

The traceroute timeout value.

**vrf** *vrf-name*

Name of the VRF. If no VRF is specified, the default-vrf is used.

## Modes

Privileged EXEC mode

## Usage Guidelines

To use the **traceroute** command on the management VRF, enter **mgmt-vrf**. You must enter the name of the management VRF manually.



## Examples

The following example executes an IPv6 traceroute, with minimum and maximum TTL values.

```
device# traceroute ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 maxttl 128 minttl 30 src-addr fec0:60:69bc:
92:205:33ff:fe9e:3f20 timeout 3

traceroute to fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470), 128 hops max, 80
byte packets
30 fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470) 2.145 ms 2.118 ms 2.085
ms
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# track (VRRP)

Enables VRRP tracking for a specified interface. VRRP Extended (VRRP-E) sessions can track a specified interface or a network.

## Syntax

```
track { ethernet slot/port | port-channel number } [ priority value ]
track network { ip-address/mask | ipv6-address/mask } [ priority value ]
no track { ethernet slot/port | port-channel number } [ priority value ]
no track network { ip-address/mask | ipv6-address/mask } [ priority value ]
```

## Command Default

The default priority value is 2.

## Parameters

### **ethernet** *slot port*

Specifies a valid, physical Ethernet subtype with appropriate slot and port number.

### **port-channel** *number*

Specifies the port-channel number. Valid values range from 1 through 6144.

### **priority** *value*

The track priority is a number from 1 through 254, and is used when a tracked interface or network up or down event is detected. For VRRP, if the tracked interface goes offline, the specified priority value is subtracted from the priority of the current device. For VRRP-E, if the tracked interface or network goes offline, the current device priority is reduced by the configured priority value. If the tracked interface or network comes online, the specified priority value is added to the priority of the current device.

### *network*

Enables tracking of a specified network. Network tracking is supported only on VRRP-E sessions.

### *ip-address*

Specifies an IPv4 network address.

### *ipv6-address*

Specifies an IPv6 network address.

### *mask*

Specifies a mask for the associated IP or IPv6 subnet.

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

This command can be used to track interfaces for VRRP or VRRP-E. Only VRRP-E sessions support network tracking.

For VRRP, the tracked interface can be any Ethernet or port-channel interface other than the one on which this command is issued.

The networks to be tracked can be either present or absent from the Routing Information Base (RIB).

The maximum number of interfaces or networks you can track per virtual router is 16.

Enter **no track** with the specified interface or network to remove the tracked port or tracked network configuration.

## Examples

To set the track port to 2/4 and the track priority to 60:

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1
device(config-vrrp-group-1)# track ethernet 2/4 priority 60
```

The following example shows how to configure network 10.1.1.0/24 to be tracked, and if the network goes down, the VRRP-E device priority is lowered by a value of 20. The lower priority may trigger a switchover and a backup device with a higher priority becomes the new master for VRRP-E group 1.

```
device# configure terminal
device(config)# protocol vrrp-extended
device(config)# interface ve 100
device(conf-if-Ve-100)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# track network 10.1.1.0/24 priority 20
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# traffic-engineering

When an MPLS-enabled device receives an IS-IS TE LSP, it stores the traffic engineering information in its Traffic Engineering database (TED). The device uses information in the TED when performing calculations to determine a path for an LSP. The user can configure the device to send out IS-IS TE LSPs for all of its MPLS-enabled interfaces.

## Syntax

```
traffic-engineering { [ isis [ level-1 | level-2 ] ] [ ospf [ area [ area_id | all ] ] ] }
no traffic-engineering { [ isis [ level-1 | level-2 ] ] [ ospf [ area [ area_id | all ] ] ] }
```

## Command Default

By default, the device does not send out IS-IS LSPs with TE extensions for its MPLS-enabled interfaces.

## Parameters

### isis

Advertise by way of ISIS.

#### level-1

Traffic-engineering for level-1.

#### level-2

Traffic-engineering for level-2.

### ospf

Advertise by way of OSPF.

#### area

designate OSPF area.

#### area\_id

Specifies OSPF area ID in IP address format.

#### all

Advertise in all OSPF areas.

## Modes

MPLS policy mode.

## Usage Guidelines

The no for of the command disables the configuration.

The user must enable the device to send out IS-IS LSPs with TE extensions when the user wants CSPF to perform constraint-based path selection because information in the TED is used to make path selections using CSPF, and information in the TED comes from IS-IS LSPs with TE extensions.

## Examples

The following example configures the device to send out IS-IS TE LSPs to the level-1 MPLS-enabled interface.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# traffic-engineering isis level-1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# traffic-engineering (LSP)

Allocating bandwidth to an LSP lets the LSRs determine how much bandwidth the LSP can consume and how much of the available bandwidth resources can be advertised.

## Syntax

```
traffic-engineering { [[ max-burst kbps ]][ max-rate kbps ]][ mean-rate kbps ]}
no traffic-engineering { [[ max-burst kbps ]][ max-rate kbps ]][ mean-rate kbps ]}
```

## Command Default

There are no allocated bandwidth allocations in the default mode.

## Parameters

- max-burst *kbps***  
Specifies the maximum burst rate in bytes. The range is from 0-2147483647.
- max-rate *kbps***  
Specifies the maximum rate in kbps. The range is from 0-2147483647.
- mean-rate *kbps***  
Specifies the average rate in kbps. The range is from 0-2147483647.

## Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp\_name*).

## Usage Guidelines

The **no** form of the command removes the traffic-engineering options.

The user can specify an average mean-rate kbps for the data on the LSP. When necessary, data can travel at max-rate Kbps, as long as the burst sent at the maximum rate contains no more than max-burst bytes.

## Examples

The following example configures the maximum rate of packets that can go through LSP *tunnel1* (in Kbps).

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# traffic-eng max-rate 20
```

The following example configures the average rate of packets that can go through LSP *tunnel1* (in Kbps).

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# traffic-eng mean-rate 10
```

The following example configures the maximum size (in bytes) of the largest burst LSP *tunnel1* can send at the maximum rate.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# traffic-eng max-burst 10
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# transit-session-accounting

Enables traffic statistics for transit sessions.

## Syntax

`transit-session-accounting`

`no transit-session-accounting`

## Command Default

By default, the command is disabled.

## Modes

MPLS policy mode.

## Usage Guidelines

Use the **no** form of the command disables the traffic statistics for transit sessions.

## Examples

The following example enables transit session accounting.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy) transit-session-accounting
```

## History

Release version	Command history
16r.1.01	This command was introduced.



# trigger

Defines event-handler triggers. When the trigger-condition occurs, a Python script is run.

## Syntax

```
trigger trigger-id [ raslog raslog-id ]
```

```
no trigger [ trigger-id ]
```

## Command Default

No trigger is defined.

## Parameters

*trigger-id*

Specifies an ID number for the trigger. Valid values are 1 through 100, and must be unique per event-handler profile.

**raslog** *raslog-id*

Specifies a RASlog message ID as the trigger.

## Modes

Event-handler configuration mode

## Usage Guidelines

You can create from 1 through 100 triggers per profile.

You can also define one trigger as part of the **event-handler** command.

To delete one or all triggers, use the **no** form of this command, as follows:

- To delete all triggers, enter **no trigger**.
- To delete a specific trigger, enter **no trigger *trigger-id***

### NOTE

You cannot delete the last remaining trigger from an activated event-handler profile.

You can modify an existing trigger without deleting it and then re-creating it.

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

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

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- In configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.

- Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

## Examples

The following example defines triggers in two event handlers.

```
device# configure terminal
device(config)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# trigger 1 raslog NSM-1001
device(config-event-handler-eventHandler2)# trigger 2 raslog NSM-1003
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# trigger-function

For an implementation of an event-handler profile, if multiple triggers are defined for an event-handler action, specifies if the action runs only if all of the triggers occur; or if one is sufficient.

## Syntax

```
trigger-function { OR | AND { time-window seconds } }
```

```
no trigger-function
```

## Command Default

The event-handler action runs if any of the triggers occur.

## Parameters

**OR**

The event-handler action runs if any of the triggers occur.

**AND**

The event-handler action runs only if all of the triggers occur.

**time-window seconds**

In seconds, specify the time window within which all of the triggers must occur in order that the event-handler action runs.

Following an initial triggering of an event-handler action, any subsequent trigger launches the action an additional time if the following conditions are true:

- The **trigger-mode** parameter is set to the default **each-instance**.
- The subsequent trigger occurs within the specified **time-window**.

## Modes

Event-handler activation mode

## Usage Guidelines

The **no** form of this command sets the **trigger-function** setting to the default **OR** option.

## Examples

The following example determines that the event-handler action runs only if all of the triggers occur within 120 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# trigger-function AND time-window 120
```

The following example resets **trigger-function** to the default **OR** option.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no trigger-function
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# trigger-mode

For an implementation of an event-handler profile, specifies if recurring trigger conditions can launch an event-handler action more than once.

## Syntax

```
trigger-mode mode
```

```
no trigger-mode
```

## Command Default

Each time the trigger condition occurs, the event-handler action is launched.

## Parameters

*mode*

Specifies if an event-handler action can be triggered only once or more than once.

**each-instance**

The event-handler action is launched on each trigger instance received.

**on-first-instance**

As long as the device is running, the event-handler action is launched only once. Following a device restart, the event-handler action can be triggered again.

**only-once**

For the duration of a device configuration, the event-handler action is launched only once.

## Modes

Event-handler activation mode

## Usage Guidelines

The **no** form of this command resets the **trigger-mode** setting to the default **each-instance** option.

## Examples

The following example sets the trigger mode to **on-first-instance**.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# trigger-mode on-first-instance
```

The following example resets **trigger-mode** to the default value of **each-instance**.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no trigger-mode
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# ttl

Configures the time to live (TTL) value for a tunnel interface.

## Syntax

`ttl ttl-value`

`no ttl`

## Parameters

*ttl-value*

Specifies the TTL value. The range is from 1 to 255.

## Command Default

The default TTL value is 255.

## Modes

Interface tunnel configuration mode

## Usage Guidelines

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

## Examples

This example configures the TTL value for the tunnel interface.

```
device# configure terminal
device (config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
device(config-intf-tunnel-5)# ttl 64
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# tx-label-silence-timer

Sets the length of the EOL transmit label silence timer for LDP-IGP synchronization.

## Syntax

**tx-label-silence-timer** *milliseconds*

**no tx-label-silence-timer**

## Command Default

The default value is 1000 milliseconds.

## Parameters

*milliseconds*

Specifies the EOL transmit label silence timer in milliseconds. Enter an integer from 100 to 60000.

## Modes

MPLS LDP EOL configuration mode

## Usage Guidelines

Use the **no** form of the resets the default value of 1000 milliseconds.

## Examples

The following example sets the length of time for the EOL transmit label silence timer to 2000 milliseconds.

```
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# eol
device(config-router-mpls-ldp-eol)# tx-label-silence-timer 2000
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# udld enable

Enables the Unidirectional Link Detection (UDLD) protocol on an interface.

## Syntax

`udld enable`

`no udld enable`

## Command Default

Disabled on interfaces by default.

## Modes

Interface configuration mode

## Usage Guidelines

Use `no udld enable` to unblock the interface if it has been blocked by the UDLD protocol.

## Examples

To enable UDLD on a specific ethernet interface:

```
device# configure terminal
deviceconfig# interface te 5/1
device(config-if-eth-5/1)# udld enable
```

# underflow-limit

Sets the underflow-limit to the input value.

## Syntax

```
underflow-limit { value }
```

```
no underflow-limit
```

## Command Default

The default is set to zero (0), meaning there is no premature adjustment because of underflow.

## Parameters

*value*

The selected number of consecutive samples which have to be below the threshold to trigger a premature adjustment.

## Modes

MPLS sub-configuration modes

config-mpls-autobw-template-template1

config-mpls-lsp-lsp1

## Usage Guidelines

The **no** function of the command sets the underflow-limit back to the default value.

## Examples

## History

Release version	Command history
16r.1.00	This command was introduced.

# unlock username

Unlocks a locked user account.

## Syntax

```
unlock username name
```

## Parameters

*name*

Specifies the name of the user account.

## Modes

Privileged EXEC mode

## Usage Guidelines

Use this command to unlock a user who has been locked out because of unsuccessful login attempts. A user account is locked by the system when the configured threshold for login retries has been reached.

## Examples

The following example unlocks a user account.

```
device# unlock username testUser  
Result: Unlocking the user account is successful
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# update-time

Configures the interval at which BGP next-hop tables are modified. BGP next-hop tables should always have IGP (non-BGP) routes.

## Syntax

```
update-time sec
```

```
no update-time sec
```

## Command Default

This option is disabled.

## Parameters

sec

Update time in seconds. Range is from 0 through 30. Default is 5 seconds.

## Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

## Usage Guidelines

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

The update time determines how often the device computes the routes (next-hops). Lowering the value set by the **update-time** command increases the convergence rate.

By default, the device updates the BGP4 next-hop tables and affected BGP4 routes five seconds following IGP route changes. Setting the update time value to 0 permits fast BGP4 convergence for situations such as a link failure or IGP route changes, starting the BGP4 route calculation in subsecond time.

### NOTE

Use the **advertisement-interval** command to determine how often to advertise IGP routes to the BGP neighbor.

## Examples

This example sets the BGP4+ update-time interval to 30.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# update-time 30
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# use-v2-checksum

Enables the v2 checksum computation method for a VRRPv3 IPv4 session.

## Syntax

```
use-v2-checksum
no use-v2-checksum
```

## Command Default

VRRPv3 uses the v3 checksum computation method.

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

Some non-Extreme devices only use the v2 checksum computation method in VRRPv3. This command enables v2 checksum computation method in VRRPv3 and provides interoperability with these non-Extreme devices.

The **no** form of this command enables the default v3 checksum computation method in VRRPv3 sessions.

## Examples

The following example shows the v2 checksum computation method enabled for an VRRPv3 IPv4 session on an Extreme device.

```
device(config)# protocol vrrp
device(config)# interface ve 100
device(config-Ve-100)# vrrp-group 10 version 3
device(config-vrrp-group-10)# use-v2-checksum
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# user (alias configuration)

Launches the user-level alias configuration mode, in which you can manage user aliases.

## Syntax

**user** *username*

**no user** *username*

## Parameters

*username*

Specifies the account login name.

## Modes

Alias configuration mode

## Usage Guidelines

To delete all aliases defined for a specified user, enter the **no** form of this command.

## Examples

The following example accesses user-alias configuration mode for the user `jdoe`, and defines a user-level alias named `sv` for the **show version** command.

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

## History

Release version	Command history
16r.1.00	This command was introduced.

# username

Creates and configures a user account.

## Syntax

```
username username password password role role_name [ access-time HHMM to HHMM ] [ desc description ] [ enable { true | false } ] [ encryption-level { 0 | 7 } ] [ expire { never | YYYY-MM-DD } ]
```

```
no username name
```

## Parameters

**username**

Specifies the account login name.

**access-time** *HHMM to HHMM*

Restricts the hours during the day that the user may be logged in. Valid values range from 0000 through 2400. By default, users are granted 24 hour access. Use 24-hour format. For example, to restrict access to the daily work schedule, use **access-time 0800 to 1800**. By default, there is no access-time limitation. To change access time, include both the new "from" time and "to" time. To restore default access time, specify **access-time 0000 to 2400**.

**desc** *description*

Specifies a description of the account (optional). The description can be up to 64 characters long, and can include any printable ASCII character, except for the following characters: single quotation marks ('), double quotation marks ("), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces, enclose the text in double quotation marks.

**enable**

Enables or disables the account.

**true**

(Default) Enables the account.

**false**

Disables the account. A user whose account is disabled cannot log in.

**expire**

Specifies the password expiration setting.

**never**

(Default) Does not specify a password expiration date.

*YYYY-MM-DD*

Specifies a password expiration date.

**password** *password*

Specifies the account password. To use the exclamation mark (!) character, either precede it with the escape character (\)—**secret!\password**—or enclose the password within double quotes—**"secret!password"**.

**role** *role\_name*

Specifies the role assigned to the username account.



**encryption-level { 0 | 7 }**

Specifies the password encryption level. The values are 0 (clear text) and 7 (encrypted). Clear text (0) is the default. If service password-encryption is enabled, it overrides a user-level setting.

## Modes

Global configuration mode

## Usage Guidelines

The *username* must be from 1 through 40 characters. It must begin with a letter or underscore and be comprised of only letters, numbers, underscore and period. A username is case sensitive. It cannot be the same as that of an existing role.

When creating a username, you must specify a password and a role. When modifying a username, it is sufficient to enter **username** *username* , followed by the new values.

The maximum number of user accounts on a device is 64.

If a user's password, access time, or role is changed, any login sessions for that user are terminated.

To specify **access-time**, use the system time defined for the Extreme operating system. For the current system time, enter **show clock**.

To delete a user, enter the **no username** *username* command.

## Examples

The following example configures a user account.

```
device# configure terminal
device(config)# username testUser password ***** role user desc
```

The following example modifies an existing user account.

```
device# configure terminal
device(config)# username testUser desc "add op test user"
```

The following example modifies an existing user account, restricting the hours that an existing user may be logged in from 08:00 AM through 18:00 PM.

```
device# configure terminal
device(config)# username testUser access-time 0800 to 1800
```

## History

Release version	Command history
16r.1.00	This command was introduced.

## vc-id

Configures a virtual connection identifier (VC ID) for a bridge domain.

## Syntax

```
vc-id id
no vc-id
```

## Command Default

A virtual connection identifier is not configured.

## Parameters

*id*  
Specifies a virtual connection identifier. The range is from 1 through 4294967295.

## Modes

Bridge-domain configuration mode.

## Usage Guidelines

For VLL, the VC ID is the VLL cross-connection instance ID.

For VPLS, the VC ID is the virtual switch instance ID.

Once a VC ID is configured for a VPLS bridge domain, it is used for all configured pseudowires (circuit emulation services).

The **no** form of the command removes the VC ID configuration.

## Examples

The following example shows how to configure a VC ID (5) for bridge domain 4.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# vc-id 5
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# vc-mode

Configures the virtual connection (VC) mode for a pseudowire (PW) profile.

## Syntax

```
vc-mode { raw | raw-passthrough | tag }
no vc-mode
```

## Command Default

The default VC mode is **raw**.

## Parameters

### raw

Specifies using raw mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the VLAN tag is removed before it is sent out on the wire. When an untagged packet is received on an untagged AC endpoint it is encapsulated as is and sent out on the wire.

### raw-passthrough

Specifies using raw-passthrough mode which enables interoperation with third-party devices. When all endpoints are configured as tagged endpoints, raw passthrough mode behaves the same way as tagged mode. When all endpoints are configured as untagged endpoints, raw-passthrough mode behaves the same way as raw mode. Select the **raw-passthrough** option, when all endpoints are configured as untagged endpoints (even when peer devices signal the PW VC mode as raw).

### tag

Specifies using tag mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the packet is encapsulated as is and sent out on the wire. When an untagged packet is received on an untagged AC endpoint, a dummy tag is added and it is sent out on the wire.

## Modes

Pseudowire-profile configuration mode.

## Usage Guidelines

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

## Examples

The following example shows how to set the VC mode to **raw-passthrough** for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# vc-mode raw-passthrough
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# virtual-ip

Configures a virtual IPv4 address or IPv6 address for the virtual router.

## Syntax

```
virtual-ip { ipv4-address | ipv6-address }
```

```
no virtual-ip { ipv4-address | ipv6-address }
```

## Parameters

*ipv4-address*

Virtual IPv4 address of the virtual router.

*ipv6-address*

Virtual IPv6 address of the virtual router.

## Modes

Virtual-router-group configuration mode

## Usage Guidelines

The virtual IPv4 address or IPv6 address is the IP address that an end-host sets as its default gateway. The virtual IP address must belong to the same subnet as the underlying interface. A maximum of 16 virtual IP addresses can be configured for VRRP; only one virtual IP address can be configured for VRRP-E. The session is enabled as soon as the first virtual IP address is configured.

You can perform this command for VRRP or VRRP-E. VRRPv3 introduced the ability to use an IPv6 address when an IPv6 VRRPv3 group is configured.

This command accepts both fe80/10 link local addresses or fe80/64 addresses as virtual-IP.

Enter the **no virtual-ip** command with a specified virtual IP address to delete the specified virtual IP address

## Examples

To assign a virtual IP address of 192.53.5.1 to the VRRP virtual group 1:

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(config-if-eth-1/6)# vrrp-group 1
device(config-vrrp-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IP address of 192.53.5.1 to the VRRP-E virtual group 1:

```
device(config)# protocol vrrp
device(config)# interface ve 20
device(config-ve-20)# vrrp-group-extended 1
device(config-vrrp-extended-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IPv6 address of 2001:2019:8192::1 to the VRRP-Ev3 virtual group 19:

```
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 2019
device(config-ve-2019)# ipv6 address 2001:2019:8192::122/64
device(config-ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)# virtual-ip 2001:2019:8192::1
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# virtual-mac

Enables generation of a virtual MAC with 0 IP hash.

## Syntax

**virtual-mac** *virtual\_mac\_address*

## Parameters

*virtual\_mac\_address*

Specifies a virtual MAC address.

## Modes

VRRP-Extended group configuration mode

## Usage Guidelines

The distributed VXLAN gateway functionality depends on VRRP-E for multi-homing. By default, the VRRP-E virtual MAC is derived as `02:e0:52:<2-byte-ip-hash>:<1-byte-vid>`. The VXLAN gateway requires that the virtual MAC be a function of only VRID. The two-byte hash of the virtual IP should be set to zeros, for example, `02e0.5200.00xx:100`.

## Examples

To enable the generation of a virtual MAC:

```
device# configure terminal
device(config)# interface ve 10
device(config-Ve-10)# vrrp-extended-group 100
device(config-vrrp-extended-group-100)# virtual-mac 02e0.5200.00xx:100
```

## History

Release version	Command history
16r.1.00	This command was introduced.

# vrrp-extended-group

Configures a virtual-router-extended group and enters into the virtual router configuration mode..

## Syntax

```
vrrp-extended-group group-ID
```

```
no vrrp-extended-group group-ID
```

## Parameters

*group-ID*

A user-assigned number from 1 through 255 that you assign to the virtual router group.

## Modes

Virtual Ethernet (ve) interface configuration mode

## Usage Guidelines

This configuration is for virtual Ethernet (ve) interfaces only.

Enter **no vrrp-extended-group** *group-ID* to remove the specific VRRP Extended group.

If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

## Examples

The following example shows how to assign the ve interface with a vlan number of 20 to the virtual router extended group with the ID of 1. (First you must enable VRRP-E on the switch.)

```
device(config)# protocol vrrp-extended
device(config)# interface ve 20
device(config-ve-20)# vrrp-extended-group 1
```

## History

Release version	Command history
16r.1.00	This command was introduced.



# vrrp-group

Configures a virtual router group (VRRP) and enters into the virtual router configuration mode.

## Syntax

```
vrrp-group group-ID [ version { 2 | 3 } ]
no vrrp-group group-ID [ version { 2 | 3 } ]
```

## Command Default

VRRP version 2 is the default.

## Parameters

*group-ID*  
A value from 1 through 255 that you assign to the virtual router group.

**version**  
Specifies in which version of VRRP the IPv4 VRRP group is to be configured.

2 | 3  
Version 2 or version 3 of VRRP.

## Modes

Interface subtype configuration mode

## Usage Guidelines

Enter **no vrrp-group** *group-ID* to remove a specific VRRP group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

You can specify in which version of VRRP the VRRP group is configured using the **version** keyword and either 2 or 3 as the version number. VRRPv3 supports both IPv4 and IPv6 addresses.

## Examples

The following example shows how to assign an Ethernet interface to the virtual router group with the ID of 1. (First you must enable VRRP on the switch.)

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(config-if-eth-1/6)# vrrp-group 1
```

The following example shows how to assign an Ethernet interface to the virtual router group with the ID of 1 for VRRPv3. (First you must enable VRRP on the switch.)

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1 version 3
```

## History

Release version	Command history
16r.1.00	This command was introduced.